



Comune di Parma

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATIVI E DELLE RISORSE INFORMATICHE, TELEMATICHE E TELEFONICHE DEL COMUNE DI PARMA

INDICE

CAPO I	4
FINALITA' – AMBITO DI APPLICAZIONE – PRINCIPI GENERALI	4
Articolo 1 – Finalità	4
Articolo 2 – Ambito di applicazione	4
Articolo 3 – Principi generali	4
CAPO II	5
POSTAZIONI DI LAVORO E CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI	5
Articolo 4 – Postazioni di lavoro	5
Articolo 5 – Corretto utilizzo e conservazione delle dotazioni di lavoro	5
CAPO III	7
CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI	7
Articolo 6 – Assistenza e interventi sulle postazioni di lavoro	7
Articolo 7 – Gestione delle password e degli account	7
Articolo 8 – Assegnazione delle credenziali al personale e agli Amministratori	8
Articolo 9 – Assegnazione delle credenziali a collaboratori/consulenti	8
Articolo 10 – Gestione delle credenziali	8
Articolo 11 – Attivazione e Revoca dei servizi del sistema Informatico	9
Articolo 12 – Disattivazione/cancellazione delle credenziali	9
Articolo 13 – Utilizzo di personal computer portatili	9
Articolo 14 – Utilizzo dei dispositivi mobili forniti dal Comune	10
Articolo 15 – Utilizzo delle stampanti e dei materiali di consumo	11
Articolo 16 – Utilizzo Telefono/VOIP	11
Articolo 17 – Lavoro a distanza	11
Articolo 18 – Utilizzo dei dispositivi non forniti dal Comune	11
CAPO IV	13
GESTIONE DELLE COMUNICAZIONI TELEMATICHE	13
Articolo 19 – Utilizzo di Internet	13
Articolo 20 – Gestione e utilizzo della posta elettronica	13
Articolo 21 – Utilizzo della posta elettronica per trasmissione dati personali	14
Articolo 22 – Recupero dei dati da parte del Comune	14
Articolo 23 – Utilizzo social media	15
CAPO V	16
SICUREZZA	16
Articolo 24 – Protezione Antivirus	16
Articolo 25 – Prevenzione degli incidenti di sicurezza	16
Articolo 26 – Gestione dei log	17
Articolo 27 – Protezione dei dati trattati senza l'utilizzo di strumenti elettronici	17
CAPO VI	18
FORMAZIONE	18
Articolo 28 – Formazione e Aggiornamento	18
CAPO VII	19
CONTROLLI E SANZIONI	19
Articolo 29 – Controlli e responsabilità	19
Articolo 30 – Sanzioni	19
CAPO VIII	20

ASSEGNAZIONE E UTILIZZO APPARATI DI TELEFONIA MOBILE	20
Articolo 31 – Assegnazione servizio telefonia mobile.....	20
Articolo 32 – Consegna servizio telefonia mobile.....	20
Articolo 33 – Ritiro/Revoca servizio telefonia mobile.....	20
Articolo 34 – Utilizzo e Custodia servizio telefonia mobile.....	21
Articolo 35 – Controlli e Verifiche	21
CAPO IX	22
DISPOSIZIONI DI RINVIO	22
Articolo 36 – Procedure operative	22
ALLEGATO A - GLOSSARIO DEI TERMINI TECNICI E INFORMATICI	23

CAPO I

FINALITA' – AMBITO DI APPLICAZIONE – PRINCIPI GENERALI

Articolo 1 – Finalità

1. Il presente Regolamento descrive le regole tecniche ed organizzative da applicare per l'utilizzo di strumentazioni informatiche che accedono al sistema informativo del Comune di Parma.
2. Ai fini del presente Regolamento si intende per "sistema informativo" il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle regole organizzative e delle procedure deputate alla acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione dei dati.
3. Le disposizioni qui contenute hanno la finalità di ottimizzare l'impiego delle risorse, introdurre regole di corretto utilizzo nel contesto organizzativo del Comune di Parma 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.
4. Quanto riportato nel presente Regolamento non esaurisce tutte le prescrizioni contenute nelle vigenti normative relativamente ad illeciti regolamentari, civili e penali, con particolare riferimento alle violazioni di sicurezza e ai reati informatici.
5. Il Comune di Parma promuove ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà del Comune.

Articolo 2 – Ambito di applicazione

1. Il presente Regolamento si applica a tutti i soggetti che utilizzano i servizi del sistema informativo del Comune di Parma il cui accesso è consentito tramite accreditamento al sistema di gestione delle identità.
2. A mero titolo esemplificativo, rientrano nel perimetro di applicazione del presente Regolamento tutti i dipendenti delle strutture e gli organi del Comune, delle Società e degli altri Enti convenzionati con lo stesso per l'utilizzo dei servizi del sistema informativo del Comune di Parma.
3. Nel seguito del Regolamento, i soggetti di cui sopra sono denominati "utenti".
4. Il presente Regolamento deve essere portato a conoscenza di tutti i dipendenti del Comune di Parma tramite i canali di comunicazione: il corso di formazione in materia di disciplina dell'utilizzo degli strumenti tecnologici fa parte del pacchetto di formazione obbligatoria per tutti i dipendenti neoassunti e si trova anche tra i materiali allegati al corso sulla Sicurezza Informatica nella piattaforma per la Formazione a Distanza del Comune (FAD).

Articolo 3 – Principi generali

1. Il Comune di Parma promuove l'utilizzo della Rete Informatica e Telematica, di Internet, della Intranet e della Posta Elettronica quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati dalla normativa vigente.
2. Ogni utente è responsabile civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi/programmi a cui ha accesso e dei dati trattati a fini istituzionali. E' altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali.
3. Sono vietati comportamenti che possono creare un danno, anche di immagine, al Comune di Parma.

CAPO II

POSTAZIONI DI LAVORO E CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Articolo 4 – Postazioni di lavoro

1. In relazione al rapporto di lavoro instaurato e alle mansioni affidate, il Comune assegna agli utenti una postazione di lavoro per l'accesso alla rete e ai servizi del sistema informativo, un insieme di dotazioni software individuali e servizi di stampa, fotocopie, scanner e telefonia con configurazione predisposta per assicurare la tutela della privacy e la riservatezza dei dati e delle informazioni trattate. Per utenti esterni che abbiano necessità di accedere ai servizi del sistema informativo del Comune di Parma, l'assegnazione di strumentazione idonea viene valutata congiuntamente dal Dirigente della struttura di assegnazione del dipendente e dalla struttura competente in materia di ICT. Ogni utente è responsabile del corretto impiego delle risorse (hardware e software) messe a sua disposizione dal Comune di Parma.
2. Le postazioni di lavoro hanno configurazioni software 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 del Comune, 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 Sistema per l'erogazione dei servizi di assistenza remota e aggiornamento automatico;
 - la possibilità di configurare parametri standardizzati ai fini di garantire la sicurezza della postazione stessa.
3. 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 dalla struttura competente in materia di ICT al fine di impedire la lettura e/o la modifica dei dati presenti a video.
4. Ogni postazione di lavoro è dotata di una configurazione base costituita dai seguenti software applicativi individuali:
 - un servizio di stampa centralizzato;
 - un antivirus locale;
 - un browser configurato centralmente per l'accesso a tutti i servizi applicativi del Comune;
 - un insieme di parametri di configurazione controllati centralmente per garantire la sicurezza della postazione di lavoro e la corretta fruibilità di tutti i servizi applicativi del Comune di Parma e di tutti i servizi Internet/Intranet;
 - un insieme di certificati di sicurezza finalizzati a garantire la sicurezza dell'utente tramite identità digitale.
5. Per i dipendenti la postazione di lavoro è inoltre dotata dei seguenti prodotti e servizi:
 - una casella di posta elettronica individuale in cloud;
 - uno spazio di archiviazione individuale in cloud;
 - telefono fisso/VOIP.
6. La postazione di lavoro è configurata e gestita centralmente dalla struttura competente in materia di ICT nel rispetto del principio di standardizzazione di tutte le postazioni di lavoro del Comune. Eventuali configurazioni ulteriori possono essere effettuate a condizione che non riducano i livelli di sicurezza applicate alla postazione di lavoro e previa autorizzazione da parte della struttura competente in materia di ICT.
7. Allo scopo di proteggere i dati personali e le postazioni di lavoro, è vietato collegare supporti rimovibili o altre tipologie di dispositivi di proprietà dell'utente alle postazioni di lavoro del Comune di Parma.

Articolo 5 – Corretto utilizzo e conservazione delle dotazioni di lavoro

1. Le dotazioni informatiche di lavoro, insieme agli accessori fisici e alle dotazioni software individuali, devono essere:
 - consegnate ad ogni nuovo dipendente con la configurazione standard di base;
 - utilizzate e conservate con diligenza al fine di ottimizzare l'impiego delle risorse del Comune;

- 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 meticolosamente insieme a tutte le altre dotazioni strumentali personali;
 - restituite immediatamente in caso di cessazione del rapporto di lavoro e/o collaborazione e in caso di assenza prolungata (esempio: congedo maternità, aspettativa, ecc); possibilmente prive di dati conservati in locale al fine di usufruire del backup automatico dei dati e delle informazioni trattate e di garantire una riduzione dei tempi e dei costi di sostituzione
2. I dati e le informazioni trattati devono essere salvati nel cloud assegnato per rendere più facile il recupero di dati e informazioni in caso di sostituzione o guasto della postazione di lavoro.
 3. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
 4. Le dotazioni restituite, ritirate per riparazione o sostituite per aggiornamento, vengono immediatamente riconfigurate in modo da cancellare ogni dato preesistente e riportate alla configurazione standard del momento. Le dotazioni riconfigurate vengono consegnate al magazzino delle dotazioni disponibili per altri utenti.
 5. L'eventuale malfunzionamento della strumentazione deve essere tempestivamente comunicato alle strutture competenti.
 6. In caso di danneggiamento della strumentazione l'utente dovrà inviare puntuale relazione sull'accaduto alla struttura competente in materia di ICT. Tale relazione dovrà essere sottoscritta dal Dirigente di riferimento che, qualora venisse accertata la responsabilità diretta del dipendente, valuterà le modalità di intervento a tutela di eventuali danni economici subiti dal Comune.
 7. E' compito del Dirigente verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato.
 8. All'utente dipendente è consentito l'utilizzo degli strumenti informatici forniti dal Comune di Parma per poter assolvere alle incombenze personali, senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali. Restano ferme le disposizioni più restrittive previste dal presente Regolamento per specifiche tipologie di strumenti (telefonia, stampa, apparati mobili).

CAPO III

CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Articolo 6 – Assistenza e interventi sulle postazioni di lavoro

1. I tecnici informatici della Società che ha in gestione e segue la manutenzione dei componenti del sistema informatico comunale possono procedere alla rimozione di ogni file o applicazione che riterranno pericolosi per la sicurezza sia sui singoli personal computer sia sulle unità di rete, previa comunicazione alla struttura competente in materia di ICT.
2. Il personale ICT del Comune e i tecnici informatici incaricati della gestione e della manutenzione del sistema informatico possono collegarsi in modalità remota alla postazione di lavoro, allo scopo di assicurare l'assistenza tecnica, la sicurezza e l'operatività, effettuando operazioni di manutenzione e aggiornamento del software installato. Gli interventi sono effettuati accedendo alla postazione con proprie credenziali. Nei casi in cui l'utente segnali malfunzionamenti per la soluzione dei quali, a scopi diagnostici, è indispensabile fare le veci dell'utente e accedere con i privilegi allo stesso assegnati, l'intervento viene effettuato, solo su specifica richiesta e autorizzazione dell'utente stesso.
3. Tutte le operazioni di collegamento remoto vengono tracciate dai sistemi informatici che registrano, in maniera non alterabile e per un limitato periodo temporale definito dalle vigenti politiche di sicurezza, le informazioni relative all'intervento effettuato.

Articolo 7 – Gestione delle password e degli account

1. L'accesso ai dati trattati con strumentazioni informatiche avviene esclusivamente previa autenticazione, ossia tramite una procedura che verifica anche indirettamente l'identità di chi vi accede.
2. L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione del Comune di Parma.
3. Le credenziali di identificazione (account) consistono in un codice per l'identificazione dell'utente (username o user id) associato a una parola chiave riservata (password), conosciuta solamente dal medesimo, oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'utente, (che può essere associato a un codice identificativo o a una parola chiave). Di seguito qualche esempio:
 - credenziali di identificazione informatica basate su parola chiave segreta: le credenziali userid+password utilizzate per l'accesso alle risorse del Comune di Parma (postazioni di lavoro, server intranet, ecc.) o per l'accesso alle applicazioni con autenticazione a un fattore;
 - credenziali di identificazione informatica basate su parola chiave segreta e one-time password (OTP): le credenziali userid+password+OTP per l'accesso alle applicazioni con autenticazione a due fattori;
 - credenziali di identificazione informatica basate su dispositivo in possesso e uso esclusivo dell'utente: le credenziali (userid+carta+pin) utilizzate per l'accesso ad aree riservate tramite smartcard (ad esempio "atti al firmatario", firma digitale ecc.).
4. Le credenziali sono costituite da uno "userid" (di norma composto da iniziale del nome e cognome separati da un punto) e da una password creata inizialmente provvisoria. L'utente viene abilitato dall'Amministratore di Dominio e, prima di poter accedere a qualsiasi risorsa informatica, deve cambiare la password.
5. Per l'accesso dell'utente ai sistemi, il Comune di Parma ha adottato l'autenticazione a più fattori (MFA) al fine di incrementare il livello di sicurezza informatica rendendo più difficile l'accesso ad eventuali utenti non autorizzati ed è parte delle azioni attivate in conformità a quanto previsto dal Regolamento generale per la protezione dei dati personali – GDPR (Regolamento UE 679/2016).
6. Fermo restando quanto previsto ai paragrafi precedenti, il Comune di Parma può adottare, quale ulteriore metodo di autenticazione, sistemi basati su *passkey*, ossia credenziali crittografiche generate e conservate su dispositivi nella disponibilità dell'utente che consentono un'autenticazione forte senza l'utilizzo di password. Le *passkey* sono considerate dispositivi di autenticazione in possesso e uso esclusivo dell'utente e devono essere impiegate nel rispetto delle politiche di sicurezza del Comune di

Parma, delle linee guida in materia di identità digitale e delle misure tecniche e organizzative previste dalla normativa vigente. L'utilizzo delle passkey è attivato e gestito dalla struttura competente in materia di ICT, che ne definisce gli ambiti di applicazione, le modalità operative e gli standard di sicurezza.

Articolo 8 – Assegnazione delle credenziali al personale e agli Amministratori

1. Il processo di rilascio delle credenziali informatiche è di competenza della struttura competente in materia di ICT del Comune di Parma a seguito di formale richiesta da parte del Settore competente in materia di Risorse Umane, per quanto concerne i servizi di dominio del Comune di Parma.
2. Il processo di autorizzazione all'accesso ai sistemi e l'assegnazione di ruoli, così come la modifica e la revoca, viene eseguito dalla struttura competente in materia di ICT a seguito di formale richiesta scritta da parte del Dirigente competente.

Articolo 9 – Assegnazione delle credenziali a collaboratori/consulenti

1. Qualsiasi collaboratore/consulente che debba accedere ai servizi di rete e di dominio direttamente presso le sedi del Comune o da remoto, deve essere accreditato tramite le credenziali informatiche il cui rilascio segue quanto indicato nel paragrafo precedente.
2. L'accreditamento dei collaboratori/consulenti avviene su richiesta del responsabile della struttura in cui tale soggetto è inquadrato. La richiesta di accreditamento dovrà riportare per ogni soggetto da accreditare i dati identificativi e la data di fine attivazione.

Articolo 10 – Gestione delle credenziali

1. Ogni credenziale di identificazione informatica si riferisce ad un singolo utente. Non è consentito l'utilizzo della stessa credenziale da parte di più utenti, fatti salvi i casi per le utenze di sistema che comunque non potranno accedere al profilo dell'utente/in sessione utente; in quest'ultimo caso la struttura di appartenenza provvede a tenere aggiornato un apposito registro con l'indicazione dei nominativi.
2. 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.
3. 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) è necessario, al primo accesso seguente al furto, cambiare la propria password e contattare il personale preposto alle problematiche di sicurezza informatica per darne immediatamente comunicazione;
 - in caso di furto o smarrimento della propria smartcard è necessario richiedere la sospensione immediata del certificato digitale al Certificatore. Si dovrà, in prima battuta, sporgere denuncia alle Autorità competenti e, successivamente, trasmettere tale denuncia al Certificatore tramite la struttura competente in materia di ICT.
4. 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 essere lunga almeno 12 caratteri in coerenza con le politiche di sicurezza del Comune di Parma e con le misure organizzative e tecniche adottate in attuazione della normativa vigente in materia di sicurezza informatica, inclusa la Direttiva (UE) 2022/2555 (NIS2). Si raccomanda inoltre di seguire 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);
 - Non deve essere uguale al nome utente;
 - Non deve essere uguale al numero di matricola;
 - Deve essere diversa dalle ultime 4 password

- 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 al Comune).

Articolo 11 – Attivazione e Revoca dei servizi del sistema Informatico

1. La richiesta di attivazione e revoca dei servizi del sistema informatico del Comune e l'installazione/rimozione dei pacchetti software è di competenza del responsabile della struttura a cui il dipendente è assegnato. Al fine di garantire la sicurezza e la responsabilità, il processo di abilitazione è tracciato in tutte le sue fasi su un sistema software del Comune di Parma ai fini dell'individuazione della responsabilità di processo. In caso di cessazione e/o cambio di struttura del dipendente i servizi assegnati in precedenza sono di norma revocati.
2. In caso di sostituzione del responsabile di una struttura, il responsabile entrante è tenuto a verificare ed eventualmente rivedere le assegnazioni di servizi a tutti i collaboratori interni ed esterni della struttura.

Articolo 12 – Disattivazione/cancellazione delle credenziali

1. Per “disattivazione delle credenziali” si intende il processo di inibizione dell'utilizzo delle credenziali e, conseguentemente, dell'accesso ai servizi di rete e di dominio del Comune.
2. Le credenziali di autenticazione assegnate a tutti gli utenti devono essere disattivate:
 - il giorno successivo alla data di interruzione del rapporto di collaborazione lavorativa con il Comune di Parma;
 - 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 privacy a seguito di adozione di apposito atto da parte del/i dirigente/i competente/i, fino alla rimozione delle cause che hanno originato il problema;
 - temporaneamente, in caso di mancato utilizzo per un periodo superiore a sei mesi.
3. La riattivazione delle credenziali può essere eseguita:
 - su richiesta dell'interessato, nel caso in cui esse siano associate a un dipendente che non ne abbia fatto uso per un periodo maggiore di sei mesi;
 - su richiesta del Dirigente competente nel caso di disattivazione temporanea disposta con atto del Dirigente medesimo.
4. La cancellazione delle credenziali deve essere effettuata:
 - decorsi 30 giorni dalla disattivazione delle credenziali nei casi di interruzione del rapporto di lavoro del dipendente con il Comune;
 - decorsi 3 giorni dalla disattivazione delle credenziali nei casi in cui il soggetto titolare delle stesse sia deceduto;
 - decorsi 3 mesi dalla disattivazione delle credenziali per inutilizzo o per sospensione nel caso di mancata riattivazione.
5. In caso di assenza del lavoro, con diritto di conservazione del posto, superiore a 6 mesi le credenziali applicative verranno disattivate. L'utente di dominio e la posta elettronica verranno mantenuti ma sarà inibito l'invio delle e-mail al di fuori del dominio comune.parma.it, fatta eccezione per specifici casi appositamente approvati dal Settore Risorse Umane.

Articolo 13 – Utilizzo di personal computer portatili

1. E' assegnato un personal computer portatile a Sindaco, Vice Sindaco, Assessori, su specifica richiesta alla struttura competente. È assegnato un personal computer a tutti i dipendenti che svolgono lavoro a distanza come previsto dal relativo Regolamento, da ultimo approvato con delibera di Giunta Comunale n. 191/2024.
2. I Dirigenti, qualora ritengano necessaria l'assegnazione di personal computer portatili da utilizzare da parte del proprio personale, inoltrano apposita richiesta motivata alla struttura competente.

3. Il dipendente custodisce il computer portatile con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di prestazione dell'attività lavorativa.
4. Il Dirigente vigila sul corretto utilizzo del personal computer da parte del dipendente. L'omessa vigilanza o negligenza può comportare in capo al Dirigente responsabilità disciplinare ed erariale in solido con il dipendente.
5. I computer portatili ad uso individuale devono essere utilizzati esclusivamente dall'utente a cui gli stessi sono stati assegnati e, qualora siano assegnati alle strutture, il loro utilizzo deve essere organizzato dalle stesse, in funzione delle proprie peculiarità ed in modo tale da garantirne il controllo.
6. L'utilizzo dei personal computer portatili richiede l'adozione di 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 del Comune di Parma 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.
7. Al fine di evitare accessi non autorizzati ai dati e ai servizi del Comune si raccomanda di:
 - provvedere al salvataggio sul proprio spazio personale in cloud di eventuali file copiati o creati in locale, rimuovendoli dal dispositivo mobile;
 - memorizzare in forma protetta i file che contengono dati personali/particolari (per es. proteggere l'accesso a cartelle o file tramite password, utilizzare appositi strumenti di cifratura concordandoli con la struttura competente in materia di ICT).
8. I dipendenti assegnatari provvedono al collegamento delle postazioni di lavoro portatili alla rete del Comune almeno una volta ogni 30 giorni per effettuare gli aggiornamenti automatici del software di controllo e sicurezza. Se l'utente assegnatario utilizza il dispositivo mobile per lavoro a distanza, lo stesso è tenuto ad osservare le disposizioni illustrate nel paragrafo relativo.
9. Per prevenire furto, danneggiamento involontario e comunque situazioni di pericolo relative all'integrità dei dispositivi e dei dati, in ragione della portabilità degli stessi, il dipendente è tenuto a custodire adeguatamente i dispositivi e non lasciarli incustoditi, neanche temporaneamente, durante i viaggi effettuati in treno o con altri mezzi di trasporto;
10. In caso di furto o smarrimento del dispositivo, l'utente è tenuto a segnalarlo tempestivamente al proprio responsabile e alla struttura competente in materia di ICT alla quale deve far pervenire copia della denuncia presentata presso le autorità competenti.

Articolo 14 – Utilizzo dei dispositivi mobili forniti dal Comune

1. I dispositivi mobili (smartphone, tablet), in ragione della loro natura, rappresentano una minaccia rilevante alla confidenzialità dei dati e delle informazioni del Comune. Specificatamente i dispositivi mobili sono soggetti a rischi specifici quali perdita di informazioni, accesso a dati "personali/particolari", facilità di furto, accesso a reti wireless non sicure, possibilità di download di app con contenuto malevolo.
2. Per ridurre il livello di esposizione alle minacce viene stabilito che:
 - Ogni dipendente che riceve in dotazione un dispositivo mobile è responsabile del suo corretto utilizzo;
 - Ogni dipendente attiva l'impostazione del blocco dello schermo dopo pochi minuti di inattività (interazione utente- device) con sblocco attraverso password;
 - È fatto divieto all'utente di installare software che comporti rischi per la sicurezza e di modificare funzionalità del sistema operativo del dispositivo mobile;
 - Al fine di evitare il furto dei dispositivi, con conseguente pericolo di accesso ai dati contenuti all'interno, il dipendente è tenuto a non lasciare incustodito il dispositivo mobile;
 - In caso di furto o smarrimento del dispositivo, il dipendente è tenuto a segnalarlo tempestivamente al proprio responsabile e alla struttura competente in materia di ICT alla quale deve far pervenire copia della denuncia presentata presso le autorità competenti.

3. L'assegnazione del servizio di telefonia mobile è regolamento dal capo VIII del presente Regolamento.

Articolo 15 – Utilizzo delle stampanti e dei materiali di consumo

1. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.
2. Tutti i dipendenti del Comune possono accedere alle stampanti/copiatrici multifunzione assegnate alla propria struttura di appartenenza. Il monitoraggio sull'utilizzo del servizio viene effettuato secondo specifici criteri previsti dal Comune per le verifiche e controlli tramite il server centrale di controllo dei servizi di stampa e copia.

Articolo 16 – Utilizzo Telefono/VOIP

1. La postazione di lavoro è di norma corredata da un dispositivo di telefonia fissa/VOIP. Le assegnazioni dei numeri telefonici, delle utenze dei software telefonici (WILDIX), degli apparati e delle abilitazioni, vengono gestite dalla struttura competente in materia di ICT.
2. L'utilizzo dei sistemi di telefonia (telefono fisso/VOIP e/o software telefonico) è riservato esclusivamente ai compiti di natura strettamente istituzionale.
3. I numeri telefonici assegnati ai dipendenti sono reperibili sul sito Intranet del Comune nella sezione "rubrica telefonica".

Articolo 17 – Lavoro a distanza

1. Ai dipendenti con rapporto di lavoro a distanza - titolari cioè di un accordo individuale di lavoro agile o di lavoro da remoto – viene fornita la strumentazione necessaria (pc portatile) per lo svolgimento delle mansioni previste.
2. La strumentazione è configurata e mantenuta dalla struttura competente in materia di ICT.
3. L'utente in lavoro a distanza è tenuto a:
 - utilizzare la strumentazione fornitagli esclusivamente per motivi inerenti all'attività lavorativa;
 - rispettare le norme di sicurezza, custodia e conservazione indicate nel presente Regolamento;
 - rispettare le disposizioni in tema di strumentazione di lavoro contenuta nel Regolamento del lavoro a distanza, vigente;
 - non manomettere in alcun modo gli apparati e l'impianto generale;
 - non variare la configurazione della strumentazione;
 - non installare software non preventivamente autorizzati;
 - non sostituirla con altre apparecchiature o dispositivi tecnologici. Per evidenti ragioni di sicurezza tale strumentazione non può essere impiegata con collegamenti alternativi o complementari a quello installato/autorizzato dal Comune di Parma ed il suo utilizzo non può essere consentito ad altri soggetti all'infuori del lavoratore.
4. Nel caso di lavoro agile, qualora il Comune di Parma non sia in grado di provvedere tempestivamente alla fornitura dell'attrezzatura tecnologica, il dipendente può utilizzare temporaneamente strumenti nella propria disponibilità, se ritenuti idonei dal Comune di Parma, in attesa della fornitura dell'attrezzatura da parte di quest'ultimo. In presenza, invece, di un accordo di lavoro da remoto, può essere utilizzata esclusivamente la dotazione informatica fornita dal Comune di Parma.
5. In caso di assegnazione della dotazione informatica l'utente è obbligato all'utilizzo anche durante lo svolgimento del lavoro a distanza.

Articolo 18 – Utilizzo dei dispositivi non forniti dal Comune

1. I soggetti accreditati al dominio del Comune di Parma hanno accesso ai servizi del Comune esposti sulla rete esterna o resi disponibili in modalità cloud, pertanto fruibili attraverso una pluralità di dispositivi. Al fine di mantenere la sicurezza dei dati di proprietà del Comune di Parma, trattati attraverso tali dispositivi, è necessario che il dipendente 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 Parma, prevenendone la memorizzazione insicura ovvero la loro trasmissione attraverso una rete insicura, dove possono essere facilmente compromessi.
2. L'utente che accede ai servizi aziendali attraverso dispositivi personali non forniti dal Comune di Parma è tenuto a:
 - non memorizzare dati del Comune sui dispositivi personali;
 - nel caso in cui i dati del Comune venissero inavvertitamente salvati sui dispositivi personali, l'utente è tenuto a cancellarli immediatamente;
 - mantenere i dispositivi personali conformi alle politiche di sicurezza definite dal Comune (ad esempio installazione dell'antivirus aggiornato, delle patch di sicurezza, ecc.)

CAPO IV

GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Articolo 19 – Utilizzo di Internet

1. L'utilizzo di Internet deve essere limitato a scopi inerenti all'attività lavorativa.
2. Il Comune di Parma si riserva di applicare profili di navigazione personalizzati per gruppi di utenti o per Settori, a seconda dell'attività professionale svolta. Attraverso tale profilazione, saranno consentite o meno le attività di navigazione a siti in modo personalizzato e correlato con la propria attività lavorativa.
3. Non è comunque consentito l'accesso, la navigazione e la registrazione a categorie di siti ritenuti non sicuri o non appropriati dal Comune di Parma, individuate attraverso un apposito sistema di URL filtering.
4. Non è consentito:
 - connettere la postazione di lavoro alla rete Internet e/o alla rete Intranet, tramite reti wifi, modem o altri apparati di accesso non espressamente autorizzati;
 - connettere alla rete interna del Comune strumenti elettronici personali o comunque non espressamente autorizzati;
 - installare e/o comunque utilizzare software di accesso alla rete Internet e/o Intranet se non espressamente autorizzati;
 - utilizzare o diffondere volontariamente programmi nocivi (per es. virus, worm, spyware, ecc.) nella rete o nei sistemi.
5. È fatto divieto di:
 - modificare le configurazioni standard del browser web fornito dal Comune;
 - accedere a caselle web mail di posta elettronica personale forniti da provider che non assicurano strumenti di protezione adeguati;
 - scaricare o eseguire alcun software o altro contenuto attivo, anche se gratuito, da siti Internet;
 - utilizzare siti pubblici di condivisione dei file e di archiviazione online non forniti dal Comune di Parma o espressamente autorizzati;
 - caricare documenti inerenti all'attività lavorativa o istituzionale, su siti pubblici di condivisione, archiviazione o backup online non forniti dal Comune di Parma o espressamente autorizzati;
 - utilizzare siti che permettano di usufruire di web proxy pubblici, aggirando l'obbligo di utilizzo del web proxy del Comune di Parma per la navigazione.

Articolo 20 – Gestione e utilizzo della posta elettronica

1. La casella di posta elettronica individuale viene assegnata ai dipendenti assunti a tempo indeterminato/determinato, agli Amministratori e ai Consiglieri Comunali.
2. La posta elettronica deve essere utilizzata esclusivamente per le specifiche finalità della propria attività lavorativa, nel rispetto della sicurezza 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 Parma.
3. E' fatto divieto di utilizzare la casella di posta elettronica per:
 - trasmissione di dati personali/particolari, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali;
 - partecipazione a dibattiti, forum, o mail-list non attinenti alla propria attività o funzione svolta per il Comune di Parma, salvo diversa ed esplicita autorizzazione.
4. Non è consentito l'invio di messaggi con allegati di dimensione superiori a 40 Mb e con estensione uguali a .lnk .bat .exe .scr ed in generale file di tipo eseguibile o di applicazione. Si precisa che il sistema di sicurezza e antivirus installato a protezione del server di posta elettronica del Comune di Parma non consente la ricezione di messaggi di posta che contengono allegati con le caratteristiche sopra elencate. Eventuali esigenze particolari potranno essere segnalate alla struttura competente in materia di ICT che individuerà la soluzione tecnica più appropriata.

5. Il dipendente è responsabile del contenuto dei messaggi inviati. Il dipendente si uniforma alle modalità di firma dei messaggi di posta elettronica di servizio individuate dal Comune di Parma. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.
6. E' vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità del Comune di Parma.
7. Nel caso in cui il dipendente reputasse opportuno, al fine di organizzare in maniera più efficiente la propria attività lavorativa, autorizzare ulteriori collaboratori (esempio gli addetti alla Segreteria) all'utilizzo della propria casella di posta elettronica, calendario, attività, note, può farne richiesta alla struttura competente in materia di ICT.
8. In caso di assenze non programmate, come ad esempio per malattia, il Responsabile della Struttura di appartenenza dell'utente assente, esclusivamente per effettiva e improrogabile necessità di assicurare continuità all'attività lavorativa, richiede al Responsabile della struttura competente in materia di ICT del Comune di Parma di attivare la funzione di delega all'accesso alla casella di posta elettronica o al cloud. L'istanza di accesso deve essere trasmessa anche in copia al dipendente assente e al delegato dallo stesso nominato. La funzione di delega rimane attiva per il tempo strettamente necessario per dare continuità all'attività lavorativa del Comune di Parma e comunque per un periodo limitato (ad esempio quello della malattia del dipendente assente) al termine del quale la funzione di delega è automaticamente disattivata.
9. In caso di assenza è necessario impostare la risposta automatica indicando un indirizzo email e/o un contatto telefonico per le segnalazioni e/o richieste urgenti.
10. In caso di cessazione del rapporto di lavoro, l'indirizzo di posta elettronica individuale dell'interessato viene mantenuto attivo, ma non accessibile, per un periodo di tempo pari a due settimane al fine di comunicare ai mittenti l'avvenuta cessazione del rapporto di lavoro.
11. Nei casi in cui il dipendente cessi il proprio rapporto di lavoro con il Comune di Parma, è concessa allo stesso la facoltà di reindirizzare per un periodo di tempo massimo di 15 giorni, i messaggi di posta elettronica ricevuti sulla casella di posta elettronica assegnata dal Comune di Parma verso altro indirizzo email, previa autorizzazione del Responsabile della struttura di appartenenza. L'utente è tenuto ad indicare l'indirizzo di posta elettronica cui reindirizzare i messaggi di posta ricevuti. Al fine di attivare questa funzione, l'utente deve effettuare istanza scritta alla struttura competente in materia di ICT.
12. Le caselle di posta elettronica certificata (PEC) non sono di norma nominative, ma assegnate alle strutture del Comune di Parma per le quali sono previsti processi di comunicazione istituzionale (ad esempio: PEC del Consiglio Comunale, PEC Del Settore Risorse Umane). La PEC istituzionale del comune di Parma è comunediparma@postemailcertificata.it.

Articolo 21 – Utilizzo della posta elettronica per trasmissione dati personali

1. La casella di posta elettronica certificata (PEC) e quella ordinaria sono mezzi attraverso i quali è possibile la trasmissione di dati personali. Nei casi in cui siano utilizzati quali mezzi per trasmettere dati personali a soggetti terzi, si rammenta che tale operazione deve essere effettuata ai sensi della normativa vigente.
2. Nei casi in cui sia necessario inviare dati personali e/o di particolari categorie e/o relativi a condanne penali e reati, verificata da parte dell'utente la liceità del trattamento ai sensi della normativa vigente, la comunicazione deve essere effettuata secondo una delle seguenti modalità:
 - utilizzando opportune tecniche di cifratura avvalendosi di strumenti preventivamente concordati con il Settore competente in materia di ICT;
 - impiegando soluzioni alternative che rendano i dati temporaneamente inintelligibili e permettano di identificare gli interessati solo in caso di necessità (per es. mandare in e-mail separate i dati di particolari categorie e/o relativi a condanne penali e reati dagli altri dati personali, utilizzare codici identificativi al posto di nome e cognome, ecc.).

Articolo 22 – Recupero dei dati da parte del Comune

1. Il recupero dei dati, in caso di assenza del dipendente, può avvenire soltanto in casi di effettiva e improrogabile necessità di assicurare continuità all'attività lavorativa. Soltanto in tale caso di emergenza è previsto l'accesso alla casella di posta elettronica e ai dati dello spazio personale del dipendente in cloud su istanza del Responsabile della struttura di appartenenza e per mezzo della struttura competente in materia di ICT. Tale procedura è finalizzata a bilanciare il diritto del Comune a garantire l'operatività organizzativa e amministrativa e l'uso consono degli strumenti forniti ai dipendenti con il diritto del lavoratore alla tutela della propria sfera di riservatezza anche nell'ambito della propria attività lavorativa.

Articolo 23 – Utilizzo social media

1. Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla Pubblica Amministrazione di appartenenza.
2. In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine del Comune di Parma o della Pubblica Amministrazione in generale.
3. Al fine di garantirne i necessari profili di riservatezza, le comunicazioni, afferenti direttamente o indirettamente il servizio, non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.
4. Tutto il personale si astiene dall'esprimere, anche nell'ambito dei social network, giudizi sull'operato del Comune di Parma derivanti da informazioni assunte nell'esercizio delle proprie funzioni che possano recare danno o nocumento allo stesso.
5. Il personale evita di postare, pubblicare o comunque esprimere considerazioni o commenti denigratori, offensivi o volgari, nei confronti delle istituzioni, dello Stato, del Comune di Parma e di coloro che li rappresentano e dei colleghi e delle colleghe; a tal proposito si intendono anche tutte le azioni di condivisione o interazione con terzi.
6. Il dipendente, nell'utilizzo dei social network, non può pubblicare immagini che lo ritraggano con simboli o fregi riconducibili al Comune di Parma, o in divisa per coloro che la indossano, se non previa autorizzazione.
7. È vietata la diffusione, in qualsiasi forma e attraverso qualunque media e social media, di informazioni confidenziali e riservate e informazioni identificative personali di cui il soggetto sia a conoscenza in ragione del proprio lavoro.
8. Il personale evita, su qualunque strumento web utilizzato, un comportamento di scherno o discriminatorio sia verso persone terze sia verso la dirigenza e verso altri dipendenti del Comune di Parma.
9. Il personale del Comune di Parma rispetta il diritto alla privacy dell'utenza dei servizi e dei colleghi, evitando di postare foto, immagini o descrizioni che non siano preventivamente autorizzate per iscritto dall'utenza dei servizi e dai colleghi. Il personale deve tenere presente che il diritto alla privacy può essere violato quando il post nel social media contiene dettagli di utenti del servizio o colleghi e colleghe tali da consentire la loro identificazione.
10. Il personale si astiene dal creare gruppi o pagine sui social che si riferiscano al Comune di Parma.
11. E' possibile la creazione di gruppi di messaggistica, utilizzati per motivi di servizio, raccomandando al personale di limitare l'utilizzo degli stessi ai soli fini istituzionali.
12. Il personale che accede a un sito di social network con un account personale per propri interessi, non accede dal luogo di lavoro e in orario di servizio e, nel caso possa essere comunque identificato dagli altri utenti dello stesso social network come dipendente pubblico, si attiene a tutte le regole del Codice di comportamento, tenendo conto che anche in contesto chiuso lo spazio virtuale è uno spazio pubblico.

CAPO V

SICUREZZA

Articolo 24 – Protezione Antivirus

1. È fatto divieto ai soggetti che sono amministratori di postazione di lavoro “personal computer” di rimuovere il programma antivirus installato su di essa e di alterarne la configurazione.
2. A seguito di segnalazione della presenza di un virus da parte del software antivirus si prescrive di:
 - sospendere ogni elaborazione e spegnere il computer;
 - segnalare l'evento alla struttura competente in materia di ICT;
 - non inviare ad altri utenti i messaggi di posta elettronica contenenti segnalazioni del virus.
3. Al fine di prevenire le minacce rappresentate da software malevoli (per es. virus, worm, spyware, ransomware ecc.) che potrebbero essere contenuti in e-mail o negli allegati delle e-mail stesse, si forniscono le seguenti indicazioni:
 - a) “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. Le operazioni di invio possono realizzarsi via email o tramite i gruppi di discussione. A titolo preventivo 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 e-mail di c.d. catene di S. Antonio, ovvero messaggi dal contenuto ambiguo che esortano ad inoltrare urgentemente delle copie ad altre persone;
 - b) Il “phishing” è una tecnica di attacco che sfrutta e-mail e siti web fantasma, del tutto simili nell'aspetto agli originali, per ingannare l'utente e carpire informazioni confidenziali o personali. È necessario, quindi, prestare massima attenzione alle e-mail 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.).
4. 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 della struttura competente in materia di ICT 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.
5. In caso di dubbi sulla qualità di messaggi e-mail, si raccomanda di seguire le indicazioni relative alla modalità di segnalazione dei messaggi sospetti fornite tramite i canali di comunicazione interna.

Articolo 25 – Prevenzione degli incidenti di sicurezza

1. Al fine di prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza nel minor tempo possibile è di enorme rilevanza operare tempestivamente e in uno spirito di collaborazione.
2. 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 di fondamentale importanza segnalare tempestivamente l'accaduto alla struttura competente in materia di ICT.
3. 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 ai dipendenti attraverso gli strumenti di comunicazione interna del Comune di Parma.

4. I sistemi informativi del Comune di Parma 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.

Articolo 26 – Gestione dei log

1. Alcune attività dei dipendenti 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.
2. Il tempo di conservazione di tutte le tipologie di log sopra elencate è definito, nel rispetto dei principi di minimizzazione e limitazione della conservazione del GDPR, in un periodo di sei mesi oppure di un periodo superiore nei casi previsti dalle normative. Ciò è motivato dalla necessità di utilizzare tali log per la verifica annuale delle attività degli amministratori di sistema prevista dal provvedimento del Garante per la Protezione dei dati personali e di avere una policy di retention dei log uniforme per tutte le tipologie, in modo da semplificare ed economizzare la gestione del sistema dei log e delle politiche di backup.
3. L'attività di raccolta e conservazione dei soli metadati/log necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica, è fissata per un periodo limitato, comunque non superiore a 21 giorni. Tuttavia, il servizio di Audit del Centro di amministrazione di Microsoft 365 (servizio attualmente in uso presso l'A.C.) ha un periodo di conservazione impostato secondo parametri predefiniti non modificabili di 90 giorni. A tale proposito, i soggetti autorizzati a gestire i log interverranno esclusivamente a fronte di richieste precedentemente autorizzate agendo su un periodo di tempo inferiore a 21 giorni dalla data della richiesta. L'eventuale conservazione per un termine ancora più ampio potrà essere effettuata, solo in presenza di particolari condizioni che ne rendano necessaria l'estensione, comprovando adeguatamente, in applicazione del principio di accountability.

Articolo 27 – Protezione dei dati trattati senza l'utilizzo di strumenti elettronici

1. 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 alle persone autorizzate al trattamento ai sensi del Regolamento (UE) 2016/679.
2. 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:
 - raccogliere prontamente, nel caso si utilizzino stampanti di rete ubicate in locali comuni (per es. corridoi), i documenti stampati - soprattutto se contenenti dati personali - in modo da preservarne la riservatezza del contenuto.
 - assicurarsi, al termine della giornata lavorativa, che i documenti contenenti dati personali o rilevanti ai fini della sicurezza del sistema informativo del Comune di Parma, non siano lasciati a vista sulla scrivania ma conservati in cassette o armadi.
 - conservare con le dovute cautele le chiavi dei cassette e degli armadi prevedendo 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, etc.).
3. 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, regolamentando 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 cassette chiusi a chiave. Al termine del trattamento, il dipendente avrà cura di ricollocare i documenti nell'archivio di provenienza.

CAPO VI

FORMAZIONE

Articolo 28 – Formazione e Aggiornamento

1. Il Comune di Parma promuove l'aggiornamento e la formazione dei propri dipendenti in merito al corretto utilizzo delle strumentazioni informatiche e telematiche in materia di sicurezza.

CAPO VII

CONTROLLI E SANZIONI

Articolo 29 – Controlli e responsabilità

1. Il Comune di Parma, attraverso i propri responsabili di struttura, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti sono stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali. In caso di uso di dispositivi elettronici personali, trova applicazione l'articolo 12, comma 3-bis del decreto legislativo 7 marzo 2005, n. 82.
2. 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.
3. I controlli sulle attività svolte mediante utilizzo dei sistemi informatici sono ammessi ed effettuati, nel rispetto dell'art. 4 della legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), nonché della normativa in materia di protezione dei dati personali, garantendo proporzionalità e minimizzazione, nei seguenti casi:
 - quando previsti da fonte normativa o regolamentare;
 - nel caso in cui si verifichino eventi dannosi o situazioni di pericolo non impediti da preventivi accorgimenti tecnici;
 - su segnalazione dell'Autorità Giudiziaria;
 - 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.
4. Nei casi in cui, a seguito di un controllo, si rilevino comportamenti illegali o non istituzionali, la struttura competente in materia di ICT può 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 al Comune di Parma;
 - 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 Dipendente, il Direttore Generale e il Segretario Generale, per i rispettivi ambiti di competenza, i quali adotteranno i provvedimenti più opportuni di cui al paragrafo successivo "sanzioni".

Articolo 30 – Sanzioni

1. La violazione dei doveri contenuti nel presente Regolamento, è fonte di responsabilità disciplinari. La violazione dei doveri è altresì rilevante ai fini della responsabilità civile, amministrativa e contabile ogni qualvolta le stesse responsabilità siano collegate alla violazione di doveri, obblighi, leggi o regolamenti

CAPO VIII

ASSEGNAZIONE E UTILIZZO APPARATI DI TELEFONIA MOBILE

Articolo 31 – Assegnazione servizio telefonia mobile

1. Il servizio di telefonia mobile si compone di SIM e apparato (cellulare, smartphone). I dispositivi assegnabili sono esclusivamente quelli disponibili nell'ambito del contratto di fornitura in vigore.
2. Il servizio di telefonia mobile è assegnato dalla struttura competente in materia di ICT del Comune di Parma sulla base di richieste degli utenti approvate dai Dirigenti dei relativi settori e motivata sulla base delle seguenti richieste di servizio:
 - soddisfare le esigenze di pronta e costante reperibilità e quelle relative a comunicazioni particolari ed indifferibili, che non possano essere svolte con gli strumenti di telefonia tradizionale o posta elettronica da postazione permanente;
 - coprire le necessità relative a servizi fuori sede e/o assistenza agli impianti;
 - rendere raggiungibile il Personale soggetto a frequenti spostamenti tra sedi diverse anche nella stessa giornata.
3. Nel caso di servizio di telefonia mobile destinato a cariche politiche, la richiesta viene avallata dal Segretario Generale.
4. La richiesta di assegnazione e la presa in carico del servizio di telefonia mobile deve essere attivata compilando la relativa modulistica disponibile sul sito INTRANET del Comune di Parma. Nel modulo è necessario specificare la tipologia di richiesta tra quelle elencate:
 - solo chiamate (servizi voce)
 - solo connessione dati (solo connettività dati)
 - chiamate e connessione dati (servizi voce e dati)
5. Il servizio di telefonia mobile può essere messo a disposizione, per esigenze di servizio, di più utilizzatori appartenenti alla medesima struttura, sulla base di assegnazioni estemporanee ("scheda a rotazione") qualora questi necessitino di utilizzare i dispositivi assegnati al Dirigente; in tal caso lo stesso Dirigente è responsabile dell'utilizzo del dispositivo e deve tenere nota degli effettivi utilizzatori per tutta la durata dell'assegnazione;

Articolo 32 – Consegna servizio telefonia mobile

1. La Struttura competente in materia di ICT del Comune di Parma, secondo la tempistica prevista dalle forniture contrattuali in essere, contatta l'assegnatario del servizio di telefonia mobile per la consegna dello stesso, la presa visione delle condizioni e la firma per accettazione delle stesse.
2. Per ogni apparato assegnato, la Struttura competente in materia di ICT deve rilevare il Numero Identificativo IMEI ed il numero della relativa SIM Card. Inoltre, la struttura competente in materia di ICT del Comune di Parma procede alla compilazione di una scheda in cui vengono riportati i suddetti, il nome e cognome dell'assegnatario del servizio, la Struttura di appartenenza, il Centro di Costo. L'assegnatario all'atto della consegna del servizio di telefonia mobile e della relativa SIM sottoscrive apposita dichiarazione di presa in carico.

Articolo 33 – Ritiro/Revoca servizio telefonia mobile

1. Qualora, per qualunque motivazione, vengano meno le esigenze per la detenzione e per l'utilizzo del servizio di telefonia mobile, deve essere inviata tempestivamente, da parte del Dirigente Responsabile, apposita comunicazione alla struttura competente in materia di ICT del Comune di Parma che provvederà al ritiro. In caso di cessazione dalla carica per qualsiasi motivo, l'Amministratore è obbligato alla restituzione del servizio di telefonia mobile alla struttura competente in materia di ICT del Comune di Parma.

2. A fronte del verificarsi delle condizioni per la revoca dell'assegnazione, al venir meno delle esigenze di servizio o in caso di violazione agli obblighi relativi all'uso e alla custodia, la struttura competente in materia di ICT del Comune di Parma provvederà al ritiro rilasciando apposita attestazione di riconsegna dello stesso e della relativa scheda SIM.

Articolo 34 – Utilizzo e Custodia servizio telefonia mobile

1. Il servizio di telefonia mobile deve essere utilizzato esclusivamente per svolgere compiti istituzionali. È di uso personale, fatto salvo quanto previsto dall'art. 31, paragrafo 6 del presente Regolamento (scheda a rotazione) e non può essere ceduto dagli assegnatari ad altri utenti dipendenti o a terzi.
2. Gli assegnatari hanno l'obbligo di mantenere il servizio di telefonia mobile in funzione durante le ore di servizio nonché in tutti i casi in cui esistano esigenze di immediata rintracciabilità.
3. In caso di malfunzionamento, l'assegnatario dell'apparato deve consegnare lo stesso alla struttura competente in materia di ICT del Comune di Parma per le opportune verifiche; la struttura competente in materia di ICT del Comune provvederà al ripristino della funzionalità dell'apparato o alla sua sostituzione.
4. L'assegnatario dei dispositivi di telefonia mobile e relativa SIM è responsabile di utilizzare e conservare con cura il dispositivo e di intraprendere ogni azione in suo potere per impedire deterioramenti o danneggiamenti dello stesso. L'assegnatario è personalmente responsabile di qualsiasi danno che possa derivare da sue azioni od omissioni, salvo il verificarsi di eventi attribuiti al caso fortuito o alla forza maggiore.
5. I dispositivi mobili, come gli smartphone, in ragione della loro natura, rappresentano una minaccia rilevante alla confidenzialità dei dati e delle informazioni del Comune di Parma, in particolare dei dati personali e delle categorie particolari di dati ai sensi della normativa vigente.
6. In caso di furto o smarrimento del dispositivo, l'utente dipendente è tenuto a segnalarlo tempestivamente al proprio responsabile e alla struttura competente in materia di ICT alla quale deve far pervenire copia della denuncia presentata presso le autorità competenti. In caso di smarrimento, l'eventuale addebito forfettario effettuato dal gestore di telefonia mobile, nei modi e termini previsti dal contratto al momento vigente, è posto a carico dell'assegnatario/utilizzatore, fino ad avvenuta denuncia di smarrimento.
7. Gli assegnatari dell'apparato di telefonia mobile di servizio sono tenuti alla piena conoscenza di tutte le funzioni e modalità descritte nei manuali di utilizzo, nonché alla conservazione degli stessi.

Articolo 35 – Controlli e Verifiche

1. Il Comune di Parma, attraverso la struttura competente in materia di ICT del Comune, nel rispetto della normativa sulla tutela della riservatezza dei dati personali, verifica il corretto uso dei servizi di telefonia mobile attraverso il riscontro con il traffico generato dalle singole utenze.
2. Qualora emergano situazioni valutate anomale dalla struttura competente in materia di ICT del Comune di Parma, la stessa provvederà, nel rispetto della normativa sul trattamento dei dati personali, a darne comunicazione tempestiva al Direttore Generale per i singoli Dirigenti, al Dirigente Responsabile per gli utenti dipendenti e al Segretario Generale per gli Amministratori.
3. Il Direttore Generale, il Dirigente Responsabile o il Segretario Generale provvedono, in forma riservata, alle necessarie verifiche, anche in contraddittorio con l'interessato, rimettendo al Sindaco la relazione conclusiva per i provvedimenti di competenza.
4. Ogni assegnatario può chiedere, in qualunque momento, alla struttura competente in materia di ICT del Comune di Parma la consistenza dei dati di traffico relativi alla propria utenza.
5. In tutti i casi in cui risultino effettivi abusi nell'utilizzo dell'apparato, che generano quindi addebiti impropri a carico del Comune di Parma, l'assegnatario dell'apparato di telefonia mobile è tenuto a

risarcire il Comune di Parma per il danno arrecato fatte salve eventuali responsabilità penali e disciplinari.

CAPO IX

DISPOSIZIONI DI RINVIO

Articolo 36 – Procedure operative

L'assegnazione del personal computer e degli apparati di telefonia mobile è regolata da procedure definite dalla struttura competente in materia ICT del Comune di Parma.

ALLEGATO A - GLOSSARIO DEI TERMINI TECNICI E INFORMATICI

Account	Iscrizione registrata su un server e che, tramite l'inserimento di una user ID e di una password, consente l'accesso alla rete e/o ai servizi. Ad esempio, un account ci permette di entrare in Internet, un altro account ci serve per ricevere e spedire posta elettronica. Un account ci consente di accedere alle risorse di una rete locale, come server, file server, stampanti. Altri account servono per accedere a server e servizi vari.
Antivirus	Tipo di software che cerca e distrugge gli eventuali programmi virus e cerca di rimediare ai danni che hanno compiuto.
Backup	Copia di riserva di disco, di una parte del disco o di uno o più file.
Browser	E' un'applicazione per l'acquisizione, la presentazione e la navigazione di risorse sul Web. Il browser utilizzato dal Comune di Parma è Edge
Cloud Computing	Modello di erogazione di servizi informatici che consente di accedere tramite Internet a risorse IT condivise.
Cyber Security	La Cyber Security è un insieme di processi, procedure e soluzioni tecnologiche in grado di proteggere la rete e i sistemi dagli attacchi digitali. La sicurezza informatica si basa sulla protezione della confidenzialità, integrità e disponibilità di un sistema informatico
Database	(Base di Dati). Qualsiasi aggregato di dati organizzato in campo (colonne) e record (righe).
Data Breach	violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato a dati personali trasmessi, conservati o comunque trattati.
Download	Registrare sul proprio disco rigido un file richiamandolo, tramite modem o rete, da un computer, da un server o da un host (tramite Internet, rete locale o geografica).
E-mail	Electronic mail, posta elettronica. Scambio di messaggi e di file attraverso una rete locale o Internet. Avviene in tempo reale ed è indipendente dalla posizione fisica dei computer mittente e destinatario. I messaggi e file vengono conservati da un server che provvede ad inoltrarli al destinatario quando questo si collega.
Firewall	Insieme di software/hardware usato per filtrare i dati in scambio fra reti diverse, al fine di proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.
Hardware	Letteralmente ferramenta, in informatica si intende l'insieme dei componenti (CPU, Hard Disk ecc.) che costituiscono un computer.
Internet	La madre di tutte le reti di computer. E' l'insieme mondiale delle reti di computer interconnesse.
Intranet	Rete locale che, pur non essendo necessariamente accessibile dall'esterno, fa uso di tecnologie Internet.
MFA	Multi-Factor Authentication – E' un metodo di autenticazione che richiede più di un fattore per verificare l'identità di un utente prima di concedere l'accesso a un sistema, servizio o applicazione.
Password	Parola che consente l'accesso di un utente ad una rete, ad un servizio telematico o ad un sito Internet. E' necessario digitarla esattamente, assieme alla user ID.
Phishing	E' un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.
Software	Sono i programmi (professionali, ludici, video, musicali, raccolte di suoni ed immagini) per i computer.
Spam (o spamming)	Invio, attraverso indirizzi generici non verificati o sconosciuti, di messaggi pubblicitari indesiderati o non richiesti, generalmente di carattere commerciale.
Streaming	Flusso di dati audio/video trasmessi da una sorgente a una o più destinazioni su Internet.
Url filtering	Sistema che permette di monitorare e filtrare la navigazione in Internet bloccando l'accesso a particolari categorie di siti al fine di limitare il rischio di utilizzo improprio della rete e la navigazione in siti non pertinenti o non compatibili con l'attività aziendale.
User ID	(O anche Nome utente) codice univoco che identifica l'utente

Utente (User)	Chiunque utilizzi un elaboratore collegato alla rete, sia che il collegamento avvenga in rete locale sia che si tratti di un accesso remoto.
Virus	Un programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi registrati.