UNIONE DEI COMUNI VALLI DEL RENO, LAVINO E SAMOGGIA
Servizio Informatico Associato

Comuni di Casalecchio di Reno, Monte San Pietro, Sasso Marconi, Valsamoggia e Zola Predosa

D.U.D.I.
Disposizioni per gli Utenti in merito all'Utilizzo delle Dotazioni Informatiche

Versione	1.2.1
Aggiornato il	26/01/2023

1. Premesse e finalità

L'Unione Reno Lavino Samoggia, i Comuni di Casalecchio di Reno, Monte San Pietro, Sasso Marconi, Valsamoggia e Zola Predosa e le Aziende AdOpera Srl e Azienda Servizi per la Cittadinanza InSieme AscInsieme (di seguito "**Titolari**") dispongono che al proprio interno vengano osservate le presenti Disposizioni per gli Utenti disciplinanti l'utilizzo delle Dotazioni Informatiche (di seguito "**DUDI"**).

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai personal computer e device mobili (come tablet e smartphone tra gli altri) e l'incremento dell'attività lavorativa in modalità smart working, espongono i Titolari a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e disciplina sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dei Titolari stessi.

Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, i Titolari adottano le presenti Disposizioni interne dirette ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e quindi del proprio sistema informatico e ad informare compiutamente gli utenti sugli specifici trattamenti dei loro dati personali che vengono effettuati e delle modalità adottate.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Regolamento Europeo n. 2016/6798 sulla protezione dei dati (da ora in poi GDPR), nonché integrano le informazioni già fornite agli interessati ai sensi dell'art. 13 del predetto regolamento, anche in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse, come previsto dall'art. 4, comma 3, dello Statuto dei lavoratori.

Tale documento sarà unico per tutti gli Enti dell'Unione in quanto la gestione delle dotazioni, degli strumenti, dei servizi informatici e della digitalizzazione della P.A. viene gestita in forma unitaria dal Servizio Informatico Associato SIA (di seguito "**SIA"**) dell'Unione in forza della convenzione associativa Rep. 19/2014.

I contenuti del DUDI inoltre sono stati determinati anche in considerazione della Circolare AGID 18 Aprile 2017, n. 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni" e sono finalizzati a rispettare tali misure come specificate nella versione 1.0 dell'allegato tecnico protocollato con numero 12165 del 21/12/2017 (e successive modificazioni), che verrà richiamato negli articoli seguenti.

Considerato inoltre che i Titolari, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, possono mettere a disposizione dei propri collaboratori che ne necessitino per il tipo di funzioni svolte, telefoni cellulari, computer portatili, tablet e smartphone, ecc., sono state inserite di seguito alcune clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

2. Entrata in vigore delle Disposizioni e pubblicità

2.1 - Con l'entrata in vigore delle presenti Disposizioni tutte le prescrizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate, qualora incompatibili o difformi, poiché sostituite dalle presenti.

2.2 - Copia del presente documento, anche per quanto prevede l'art.7 della Legge n. 300/1970 (Statuto dei lavoratori), verrà diffuso con le seguenti modalità:

a) neo assunti: allegato al contratto di lavoro;
b) altri dipendenti: trasmesso via email e sempre a disposizione sulla sezione del Servizio Personale Associato contenente tutti i documenti di interesse dei dipendenti;
c) soggetti esterni che erogano servizi a favore dei Titolari: allegato a contratti di appalto che implichino l'utilizzo e/o l'accesso alla infrastruttura dell'Unione;
d) soggetti esterni istituzionali (es Città Metropolitana, forze dell'ordine etc): mediante trasmissione via email;
e) soggetti non istituzionali (es associazioni, start up, tirocinanti o altri utenti sporadici) che per diversi motivi utilizzino dotazioni informatiche all'interno delle sedi dell'Unione: allegato a nuovi contratti/convenzioni e, negli altri casi, trasmesso via email;

Pertanto, le presenti Disposizioni entrano a far parte, per quanto occorra, del Codice disciplinare aziendale.

Tale documento entrerà in vigore in seguito alla sua approvazione da parte delle Giunte

3. Ambiti di applicazione

3.1 - Le disposizioni contenute in questo documento si applicano:

- a tutti i dipendenti, senza distinzione di ruolo e/o livello
- a tutti gli amministratori (Sindaco, Assessori, Consiglieri)
- a collaboratori e consulenti dei Titolari a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori coordinati e continuativi, in stage, prestatori d'opera intellettuale, prestatori di servizi etc.) che venissero autorizzati a far uso di strumenti tecnologici dei Titolari o perfino di accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati.

Pertanto, le disposizioni di seguito previste devono intendersi a carico di tutte le figure sopra elencate, ferma restando la necessità che se ne dia opportuna conoscenza con le modalità di cui al punto 2.2.

3.2 - Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve così intendersi ogni dipendente, amministratore (Sindaco, Assessore, Consigliere), collaboratore e/o consulente (come sopra già precisato) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "responsabile esterno del trattamento" o "terzo", ai sensi dell'art. 4 comma 10 del GDPR, in ragione delle attività e degli impegni che si assume nell'organizzazione aziendale o a favore dei Titolari stessi.

3.3 - Per quanto attiene gli amministratori, si precisa che nei loro confronti non valgono le disposizioni che secondo la normativa possono essere applicate solo in quanto collegate allo status di dipendente, tra cui si evidenziano a titolo esemplificativo e non esaustivo quelle inerenti la navigazione internet (art. 10), la partecipazione ai social media (art. 14) e le sanzioni (art.19)

3.4 - Modalità di lavoro in smart working: per le prestazioni lavorative eseguite con la modalità di lavoro denominata "Smart Working" si rimanda nello specifico all'art. 18 precisando che il contenuto del DUDI si intende vincolante anche per i lavoratori in Smart working ad eccezione delle disposizioni che confliggono con quanto stabilito al citato art. 18

3.5 - Modalità di lavoro flessibile: per le prestazioni lavorative eseguite al di fuori dell'orario di lavoro e al di fuori di una sede dell'Unione, denominata "Flessibile" si rimanda nello specifico all'art. 18 precisando che il contenuto del DUDI si intende vincolante anche per i lavoratori in modalità flessibile ad eccezione delle disposizioni che confliggono con quanto stabilito al citato art. 18.

4. Utilizzo dei personal computer aziendali

4.1 - I personal computer aziendali, fissi o notebook, d'ora in avanti riferiti come PC, affidati all'utente sono degli strumenti di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. I PC devono essere custoditi con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.

4.2 - I PC dati in affidamento all'utente permettono l'accesso alla rete dei Titolari solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 5.

4.3 - I Titolari rendono noto che il personale incaricato che opera presso il servizio SIA è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dei Titolari, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il servizio SIA ne darà comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso.

4.4 - Il personale incaricato del servizio SIA ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato su chiamata dell'utente o a seguito di rilevazioni di problemi tecnici del sistema informatico/telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione preventiva della necessità dell'intervento stesso.

4.5 - Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del servizio SIA per conto dei Titolari, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno o scaricati dalla rete, sussistendo in tali casi il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione può esporre i Titolari a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico dei Titolari, come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.

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

4.7 - Ogni utente deve prestare la massima attenzione ai supporti e periferiche di origine esterna (hard-disk, DVD, fotocamere, apparati multimediali, ecc ...), avvertendo immediatamente il personale del servizio SIA nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 11) relativo alle procedure di protezione antivirus.

4.8 - Ogni utente che dovrà, per qualsiasi motivo, lasciare incustodita temporaneamente la propria postazione di lavoro, sarà tenuto a bloccare l'accesso alla propria sessione tramite un sistema di blocco del sistema operativo che richieda l'inserimento della password di accesso per effettuare l'operazione di sblocco. I PC dotati di sistema operativo Windows appartenenti al sistema informatico dell'Unione prevedono un sistema di blocco automatico della sessione utente che si attiva autonomamente dopo 15 minuti di inattività. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

4.9 - I PC devono essere spenti ogni sera al termine dell'attività lavorativa, anche in caso di attività svolta al di fuori della sede di lavoro, o in caso di assenze prolungate o in caso di suo inutilizzo. Tale modalità permette di evitare cospicui sprechi di energia elettrica ed ai software antivirus e altri software dediti alla sicurezza dei pc di poter effettuare aggiornamenti ed operazioni che richiedono un riavvio. Eventuali eccezioni vanno segnalate e concordate con il servizio SIA. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso (si faccia riferimento al punto 4.8).

5. Gestione delle password e degli account

5.1 - Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del servizio SIA, previa apertura di un ticket di assistenza (secondo le indicazioni di cui al punto 12) da parte del Dirigente/Responsabile del servizio indicante l'ambito nel quale verrà inserito ed andrà ad operare, il nuovo utente.

5.2 - Le singole credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal SIA, associato ad una parola chiave (password) riservata che dovrà venir **custodita dall'incaricato con la massima diligenza e non divulgata**. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del servizio SIA.

5.3 - Le credenziali di autenticazione si distinguono tra:

A. password di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete (accesso al PC)

B. password per l'accesso ai singoli applicativi (software)

Il SIA è impegnato a far convergere in maniera automatica le password degli applicativi (punto B) con la stessa della rete (punto A) in modo da semplificare la gestione degli account da parte degli utenti e di uniformare le modalità di gestione delle stesse password (come previsto al successivo punto 5.4).

5.4 Le password devono sempre rispettare le seguenti condizioni:

- deve avere un lunghezza minima di 10 caratteri
- non deve contenere il nome dell'account dell'utente o parti del nome completo dell'utente che superano due caratteri consecutivi
- deve contenere almeno 3 caratteri delle 4 categorie:
    - una lettera maiuscola (dalla A alla Z)
    - una lettera minuscola (dalla a alla z)
    - un numero (da 0 a 9)
    - un carattere non alfanumerico (per esempio: !, $, #, %, _, & ecc.)

La password deve essere modificata al primo utilizzo e periodicamente ogni 90 giorni ai sensi della normativa in vigore, secondo la procedura di modifica proposta automaticamente all'utente. Non si potranno inoltre ri-utilizzare le precedenti 5 password.

La password, inoltre, non deve contenere riferimenti agevolmente riconducibili all'utente (es. data di nascita, nome di familiari etc).

5.4 - Le password devono essere personali e segrete e non devono essere comunicate o cedute a nessuno.

5.5 - Non è consentito effettuare l'accesso ad una qualunque dotazione informatica con le credenziali personali di accesso di un altro utente.

5.6 - Non è consentito l'uso di credenziali di accesso "generiche" non riconducibili ad una singola persona per effettuare l'accesso ad una qualunque dotazione informatica. Eventuali casi particolari andranno eventualmente concordati tra il Dirigente/Responsabile di servizio richiedente ed il servizio SIA.

5.7 In caso di cessazione del rapporto di lavoro, tutti gli account individuali dell'utente verranno immediatamente sospesi e, dopo dieci giorni lavorativi dalla data di cessazione, dismessi a meno di una richiesta effettuata tramite l'apertura di un ticket di assistenza (secondo le indicazioni di cui al punto 12) da parte del Dirigente/Responsabile di servizio, in accordo con il soggetto che termina il rapporto di lavoro, in cui viene concordato e stabilito la data di dismissione dei singoli account. Le modalità di sospensione e cancellazione delle caselle di posta elettronica individuali vengono specificate nel punto 9.15.

6. Utilizzo delle periferiche, delle cartelle condivise e della rete informatica

6.1 - Per l'accesso alla rete dei Titolari ciascun utente deve utilizzare le proprie credenziali di autenticazione.

6.2 - Per cartella condivisa (unità di rete) si intende uno spazio disco disponibile sui server centrali, per la memorizzazione di dati e programmi accessibili ad un gruppo di utenti preventivamente autorizzati.

6.3 - Le cartelle presenti nei server dei Titolari sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e backup da parte del personale del servizio SIA. Si ricorda che tutti i dischi o altre unità di memorizzazione locali - es. disco C: interno al PC - non sono soggetti a salvataggio da parte del personale incaricato del servizio SIA. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

6.4 - Risulta opportuno che ciascun utente, provveda alla pulizia periodica (almeno ogni tre mesi) di tutti gli spazi assegnati, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati al fine di evitare, salvo casi eccezionali, un'archiviazione superflua.

6.5 - Il personale del SIA può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

6.6 - Nella gestione dei sistemi informatici aziendali, il SIA potrà acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, ad esempio, le informazioni sugli orari di accensione e spegnimento dei PC rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate, ai sensi del successivo punto 15.2), per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente punto 4.3), e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

6.7 - L'utente deve attenersi ad usare un metodo di archiviazione di file e cartelle consono, non creando un numero di livelli di sottocartelle superiore a 11 e utilizzando nomi di file e cartelle che non superano singolarmente i 20 caratteri, in modo che l'intero percorso del singolo file non superi i 260 caratteri. Il non rispetto del metodo soprastante può portare a comportamenti anomali sulle operazioni comuni che vengono effettuate su file e cartelle (apertura, rinomina, copia e incolla, taglia incolla, ripristino, ecc)

6.8 - Ogni Ente ed Azienda può disporre di alcune unità di rete condivise:

A. Unità **Servizi,** lettera **Q:**, contenente le directory dei singoli servizi accessibili solamente al Dirigente/Responsabile di servizio e del relativo personale.
B. Unità **Tutti**, lettera **R:** Risulta essere uno spazio condiviso da tutti o parte degli utenti del singolo Ente/Azienda. E' prevista la progressiva dismissione delle unità Tutti, viste le relative problematiche di privacy e di condivisione di dati personali, che verranno sostituite da una gestione di cartelle condivise puntualmente con i soli soggetti interessati. Tali cartelle condivise verranno create dal servizio SIA in seguito all'apertura di un ticket di assistenza (secondo le indicazioni di cui al punto 12)
C. Unità **Software**, lettera **P:** Risulta essere uno spazio condiviso gestito dal servizio SIA per l'uso di particolare software che non deve essere utilizzato come spazio di archiviazione.

6.9 - Ogni utente può disporre di una cartella di rete privata identificata con il proprio username e dalla lettera **U:** nella quale solo il singolo utente dispone dei diritti di accesso. Per tale ragione tale cartella non deve essere dedicata ad archiviare documenti di interesse dell'intero servizio. Per tale cartella privata valgono gli stessi principi dei punti 6.3 e 6.4.

6.10 - L'accesso alle unità di rete da parte degli utenti ed ogni successiva modifica, deve essere autorizzato dal Dirigente/Responsabile del servizio tramite l'apertura di un ticket di assistenza secondo le indicazioni del paragrafo 12, specificando le cartelle per le quali si richiede l'accesso.

7. Utilizzo di altri dispositivi elettronici

7.1 - **Tutti i dispositivi elettronici dati in dotazione al personale dai Titolari devono considerarsi strumenti di lavoro**: ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative. Fra i dispositivi in questione vanno annoverati i telefoni fissi, PC portatili, tablet, telefoni cellulari, smartphone, stampanti, scanner etc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete dei Titolari o di condividere documenti, dati e materiali ivi conservati e/o trattati.

7.2 - Dispositivi elettronici personali: con riferimento all'uso dei seguenti dispositivi mobili elettronici personali: telefoni smartphone e tablet, quando lo richiedano esigenze connesse alla tipologia di lavoro, è consentito l'uso di dispositivi personali per finalità lavorative esclusivamente per l'accesso alla suite Google Workspace nel rispetto delle seguenti prescrizioni:

- i dispositivi personali dovranno non essere liberamente accessibili ma bloccati con il più efficace tra i seguenti sistemi di protezione disponibile sul dispositivo utilizzato (in ordine di efficacia): PIN, impronta digitale, riconoscimento facciale;
- non è consentito salvare file / allegati sui propri dispositivi (con particolare riferimento a documenti contenenti dati personali);
- il dispositivo personale dovrà essere ad uso esclusivamente personale e quindi non in condivisione con altre persone

7.3 - L'utente resta responsabile dei singoli dispositivi assegnati che devono custodire con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni. In caso di smarrimento o furto di dispositivi le cui memorie possano essere cancellate o bloccate da remoto a cura del servizio SIA per evitare sottrazioni o diffusioni di dati incontrollati, l'utente dovrà immediatamente avvisare il servizio SIA, e comunque al massimo entro 24 ore dal fatto.

7.4 - Con riferimento ai telefoni aziendali e telefoni cellulari/smartphone, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, viene consentita solo nel caso di comprovata necessità ed urgenza. Inoltre, l'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è consentito nei seguenti casi:

- assegnazione di telefono aziendale DUAL SIM
- assegnazione di telefono aziendale con singola SIM aziendale con ripartizione spese per chiamate personali
- assegnazione di SIM aziendale installata su telefono personale (DUAL SIM)

Nei casi di uso promiscuo sopra indicati, valgono le prescrizioni in materia di sicurezza indicate nel presente capitolo.

7.5 - Si precisa, peraltro, che le disposizioni previste nel presente documento ai punti 4), 8), 9), 10), 11) e 14) dello stesso trovano applicazione anche nell'uso dei dispositivi elettronici qui considerati.

7.6 Viene infine disposto il divieto di utilizzo per fini personali di fax aziendali, per spedire o per ricevere documentazione, e/o di fotocopiatrici aziendali, salva diversa esplicita autorizzazione da parte del Dirigente/Responsabile di servizio.

7.7 - Il Dirigente/Responsabile di servizio si impegna ad eliminare, ove è possibile, le periferiche personali in favore di quelle di rete (periferiche condivise), che permettono un risparmio nei costi di gestione, limitando le periferiche personali esclusivamente ai casi in cui sia indispensabile per ragioni di servizio o di riservatezza (per periferica condivisa si intende stampante, scanner, plotter o qualsiasi altro dispositivo elettronico che può essere utilizzato in contemporanea da più uffici).

7.8 - Il Dirigente/Responsabile di servizio vigila sul corretto utilizzo dei device portatili e ne è corresponsabile assieme al lavoratore che deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nei luoghi di lavoro.

7.9 - I lavoratori a cui vengono dati in dotazione uno o più device portatili, devono abilitare, accettare ed effettuare nel minor tempo possibile gli aggiornamenti di sistema che il device propone e segnala.

7.10 - I device portatili non sono cedibili a terzi estranei all'Ente e devono essere utilizzati ai soli fini istituzionali.

7.11 - In caso di perdita o smarrimento di un device aziendale o personale - ma che sia comunque utilizzato per visualizzare dati aziendali (telefono o mail) la persona a cui è affidato o è titolare del dispositivo ha l'obbligo di presentare denuncia all'Autorità Giudiziaria e dare tempestiva comunicazione al SIA e al Comune che ha attribuito il device, per gli adempimenti conseguenti allo smarrimento.

7.12 - Si definiscono invece device portatili personali, qualunque device che non sia di proprietà di uno dei Titolari. Con riferimento ai device personali, non sono consentite:

- le connessioni a qualunque presa di rete delle presenti nelle reti cablate dei Titolari
- le connessioni ai pc di di proprietà dei Titolari di qualunque device portatile personale

E' assolutamente vietata la connessione a prese di rete o pc di proprietà dei Titolari di qualunque dispositivo portatile di provenienza sconosciuta o di proprietà di cittadini.

In caso di eventi pubblici, presentazioni, talk in cui è necessario la trasmissione o proiezione video di materiale digitale/informatico (es: presentazioni Power Point) proveniente da relatori esterni ai Titolari, si richiede l'invio preventivo dello stesso materiale.

8. Utilizzo e conservazione dei supporti rimovibili

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

8.2 - L'utente resta, in ogni caso responsabile della custodia dei supporti e dei dati aziendali in essi contenuti; in particolare, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

8.3 - E' vietato l'utilizzo di supporti rimovibili personali (es. chiavette USB). Per la condivisione o la visualizzazione di documenti fuori delle sedi di lavoro si consiglia fortemente l'uso di Google Drive facente parte della piattaforma Google Workspace in dotazione a tutto il personale. In casi di comprovata necessità, supporti rimovibili (non personali ma consegnati dall'Ente) potranno essere utilizzati. Resta fermo il divieto di utilizzare tali supporti per fini personali caricando file non attinenti l'attività lavorativa.

8.4 - Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del servizio SIA e seguire le istruzioni da questo impartite. Nel caso di dispositivi elettronici, con riferimento in particolare a PC portatili, tablet ed altri dispositivi sui quali possono venire salvati documenti, dati ed altro materiale, dovrà porsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo, concordata comunque ogni opportuna azione al riguardo con il personale del servizio SIA.

9. Gestione ed utilizzo della posta elettronica ed altri strumenti di condivisione documenti

9.1 - La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

9.2 - È fatto divieto di utilizzare le caselle di posta elettronica aziendale per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del servizio SIA. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

9.3 - La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili, obsoleti o non costituenti corrispondenza lavorativo/istituzionale e soprattutto allegati ingombranti. Si sottolinea infatti che la casella di posta elettronica è uno strumento di lavoro e non un archivio documentale.

9.4 - È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo. In caso di dubbi non si deve procedere all'apertura di allegati ma contattare il servizio SIA per chiarimenti.

9.5 - Ogni servizio può essere dotato di una casella di posta elettronica di servizio o di un gruppo di posta elettronica. Tale scelta viene concertata tra il Dirigente/Responsabile ed il servizio SIA valutando gli aspetti tecnici, organizzativi ed economici e poi formalizzata tramite l'apertura di un ticket di assistenza secondo le indicazioni del paragrafo 12.

9.6 - Una casella di posta elettronica di servizio risulta essere una casella di posta a tutti gli effetti cui si deve accedere tramite il sistema di "delega" gestito dal sistema di posta elettronica.

Un gruppo di posta elettronica di servizio, invece, risulta essere un indirizzo di posta elettronica che semplicemente consegna tutte le email ricevute dal gruppo alle caselle di posta individuali dei componenti del gruppo stesso.

9.7 - La creazione, la cancellazione e le relative autorizzazioni di accesso ad una casella di posta elettronica di servizio e/o l'appartenenza ad un gruppo di posta elettronica di servizio devono essere autorizzate dal Dirigente/Responsabile tramite l'apertura di un ticket di assistenza secondo le indicazioni di cui al punto 12).

9.8 - Nel caso in cui venisse assegnato all'utente anche la gestione di uno o più indirizzi di posta elettronica certificata di cui i Titolari si fossero dotati, tale utente dovrà attenersi alle disposizioni previste nell'eventuale ulteriore apposito Regolamento aziendale a ciò dedicato e che va comunque a completare ed integrare il presente documento.

9.9 - Al fine di garantire la continuità dell'attività lavorativa, in caso di assenza programmata e prolungata (ad es. per ferie), gli utenti sono tenuti ad utilizzare l'apposita funzionalità di sistema "Risponditore automatico" che invia automaticamente al mittente un messaggio di risposta, avvisando dell'assenza del destinatario del messaggio e relativo periodo e indicando eventuali modalità alternative per contattare la struttura.

9.10 - La gestione delle caselle di email avviene in modo centralizzato sulla piattaforma cloud denominata Google Workspace di Google. L'accesso a tali caselle avviene mediante l'utilizzo del browser di navigazione. Per tutte le applicazioni della piattaforma Google Workspace (Google Gmail, Google Drive, Google Calendar, ecc) viene consigliato ed incoraggiato l'uso del browser Google Chrome o, in alternativa, Mozilla Firefox.

9.11 - Tutti i titolari di account istituzionale Google Workspace, dotati di dispositivo mobile aziendale (smartphone o tablet), e tutti i dirigenti e titolari di posizione organizzativa, indipendentemente dalla disponibilità di dispositivo mobile aziendale, devono abilitare il sistema di "verifica in più passaggi" (o autenticazione a più fattori) che permette di aggiungere un ulteriore livello di sicurezza alla fase di accesso al proprio account.

Per tutti gli altri è fortemente raccomandata l'abilitazione dello stesso sistema di verifica in più passaggi, la quale:

- oltre ad essere a tutela dell'Ente è anche finalizzato alla tutela degli stessi dipendenti
- anche in caso di utilizzo di dispositivo mobili personali per l'autenticazione (ricezione sms, notifica push etc) non comporta costi aggiuntivi o trattamento dati personali per finalità diversa da quelle della semplice autenticazione

9.12 - Non è consentita l'installazione e l'uso di client di posta elettronica nei PC (es. Microsoft Outlook, Mozilla Thunderbird), salvo che per specifiche esigenze concordate con il servizio SIA.

9.13 - La gestione delle caselle di email nei device mobili, smartphone e tablet, di servizio, deve avvenire tramite le app ufficiali Google (presenti negli store Google Play, Apple Store e/o negli store dei singoli produttori dei device) se compatibili con il device. In caso di non compatibilità, l'utente può richiedere, tramite l'apertura di un ticket di assistenza secondo le indicazioni di cui al punto 12), la consulenza del servizio SIA per individuare il client di posta migliore per il singolo device.

9.14 - Ogni Ente afferente all'Unione può disporre di due gruppi di posta elettronica:

- **dipendenti@...** le email indirizzate a questo gruppo verranno ricevute solamente da tutti gli utenti che sono dipendenti di quel certo Ente
- **tutti@...** le email indirizzate a questo gruppo verranno ricevute da tutti gli utenti che hanno un indirizzo email con il dominio dell'ente (es: @comunexyz.bo.it). Nel caso di un Comune questo permetterà di raggiungere anche gli Amministratori che hanno la casella di posta elettronica istituzionale ed eventuali account di servizio

Entrambi vanno utilizzati **solo** per comunicazioni di servizio e/o istituzionali. I gruppi per invio massivo di email sono verificabili al link sottostante:
https://sites.google.com/unionerenolavinosamoggia.bo.it/ucrls-sia/documentazione/gruppi-liste-distribuzione

L'utilizzo di questi indirizzi deve sempre essere preventivamente comunicato/autorizzato dal proprio Responsabile di servizio.

In caso di invio agli indirizzi sopra indicati di comunicazioni istituzionali, è fatto divieto per i destinatari di utilizzare l'opzione "rispondi a tutti", rimanendo possibile per eventuali chiarimenti rispondere solo al mittente dell'email

9.15 - In caso di cessazione del rapporto di lavoro:

A. la casella di posta individuale dell'utente verrà immediatamente sospesa il primo giorno della data di cessazione.
B. al decimo giorno lavorativo successivo alla data di sospensione (coincidente alla data di cessazione del rapporto di lavoro come al punto 9.15.A), a meno di una richiesta tramite l'apertura di un ticket di assistenza, (secondo le indicazioni di cui al punto 12) da parte del corrispettivo Dirigente/Responsabile di servizio in accordo con il soggetto che termina il rapporto di lavoro, in cui viene concordato e stabilito la data di

dismissione dei singoli account, verrà effettuato un backup della casella e la stessa verrà cancellata definitivamente. Tale backup verrà eliminato definitivamente dopo esattamente 1 anno dalla data di effettuazione dello stesso.

C. almeno quindici giorni prima della sospensione dell'account (coincidente alla data di cessazione del rapporto di lavoro), l'utente della casella dovrà attivare una risposta automatica in cui dovrà indicare
    a. data di cessazione del rapporto di lavoro
    b. indirizzi email e contatti alternativi per le finalità di servizio
D. non è consentito disporre (né richiedendo al servizio SIA né in autonomia) l'inoltro automatico dei messaggi delle casella di posta dell'utente cessante verso nessun'altra casella o gruppo di posta elettronica, in ottemperanza al provvedimento del Garante della Privacy 456 del 2015.

9.16 - Si sottolinea che i punti sopra elencati del presente paragrafo 9 per la posta elettronica, vanno considerati vigenti anche per l'utilizzo dei servizi compresi nella stessa suite di prodotti G-Suite (es: Google Drive, Google Calendar, Google Site, ecc) tramite i quali gli utenti possono condividere informazioni e documenti informatici inerenti la propria attività lavorativa.

E' espressamente vietato utilizzare gli strumenti di condivisione di Google Drive per pubblicare documenti direttamente sul web. In caso di necessità, prima di procedere, è obbligatorio ricevere l'autorizzazione da parte del proprio Dirigente/Responsabile.

10. Utilizzo e navigazione in Internet

10.1 - **I PC assegnati al singolo utente ed abilitati alla navigazione in Internet sono strumenti aziendali utilizzabili esclusivamente per lo svolgimento della propria attività lavorativa**. È quindi proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

10.2 - In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica ad esempio) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del servizio SIA);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Dirigente/Responsabile di servizio e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'iscrizione con account aziendale e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nickname) se non espressamente autorizzati dal Responsabile d'ufficio;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

10.3 - Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Titolari rendono peraltro nota l'adozione della presenza di specifici sistemi di blocco e/o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una serie di "black list".

10.4 - Gli eventuali controlli, compiuti dal personale incaricato del servizio SIA ai sensi del precedente punto 4.3), potranno avvenire mediante sistemi di controllo dei contenuti o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre dodici mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dei Titolari.

10.5 - L'accesso da remoto alla rete aziendale è possibile agli utenti abilitati solo a seguito di comunicazione di specifiche credenziali o dell'installazione di software che lo abilita sui dispositivi in uso in seguito ad una richiesta da parte del Dirigente/Responsabile di servizio al servizio SIA tramite l'apertura di un ticket di assistenza secondo le indicazioni di cui al punto 12).

L'accesso da remoto alla rete aziendale è possibile solo utilizzando dispositivi aziendali autorizzati. A tale scopo vengono svolti controlli automatici che possono impedire l'accesso utilizzando dispositivi non abilitati.

11. Sicurezza informatica: antivirus, anti malware, phishing

11.1 - Il sistema informatico e la piattaforma Google Workspace dei Titolari sono protetti da software antivirus e antimalware continuamente aggiornati. Ogni utente deve comunque mantenere sempre alta l'attenzione e tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo che possono portare ad una o più delle seguenti casistiche/conseguenze fraudolente e pericolose seguenti (non esaustive):

- blocco del singolo dispositivo
- blocco dell'intera o parte dell'infrastruttura informatica dei Titolari
- furto di credenziali e/o accesso indebito ai servizi e/o infrastruttura informatica dei Titolari
- truffe ai danni dei Titolari
- data breach relativi a furto ed esfiltrazione di dati fuori dell'infrastruttura informatica dei Titolari
- data breach relativi alla criptazione dei dati o in generale all'inibizione da parte dei Titolari della disponibilità di parte o di tutti i dati
- estorsioni e/o richieste di riscatto relative ad una o più delle precedenti casistiche

11.2 - Nel caso il software antivirus rilevi la presenza di un virus o di un malware, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale del servizio SIA tramite telefonata ai tecnici o, in caso di mancata risposta, tramite l'apertura di un ticket di assistenza secondo le indicazioni del paragrafo 12.

11.3 - Ogni dispositivo rimovibile e/o magnetico di provenienza esterna ai Titolari dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del servizio SIA.

11.4 - Ogni utente deve porre la massima attenzione alla gestione della posta elettronica, su tutte le caselle di posta a cui si ha accesso, gestione, delega, che sia posta elettronica "standard" o certificata (PEC). Tale attenzione deve essere massima anche quando la gestione della posta elettronica viene effettuata tramite software che "scaricano" e gestiscono messaggi di posta elettronica "standard" o certificata (PEC), come a titolo di esempio, nei software gestionali di Protocollo Informatico. Tutte le caselle di posta elettronica "standard" o certificata (PEC) dei Titolari, nessuna esclusa, sono costantemente obiettivi di pericolosi tentativi di phishing o di altri tipi di attacchi informatici, tramite ad esempio, la presenza di link o allegati malevoli, atti ad ottenere una o più casistiche/conseguenze elencate nel punto 11.1.

Ogni utente è tenuto a:

- **esaminare attentamente le email sospette per controllare la presenza di indizi rivelatori di phishing, come grammatica scadente, loghi sgranati o link fasulli**
- **non aprire link o allegati senza controllare in maniera preventiva il vero indirizzo email del o dei mittenti**
- **in caso di un minimo dubbio non aprire link o allegati, NON INOLTRARE email sospette al SIA nè a nessun altro ma si proceda ad aprire un ticket al SIA secondo le indicazioni del paragrafo 12 (SENZA allegare la mail nel ticket) lasciando un contatto telefonico per essere ricontattati da un tecnico SIA.**
- **se per errore è stato effettuato un clic su un link di phishing, non deve inserire alcun dato e deve chiudere la pagina web che è stata aperta**

11.5 - Il servizio SIA predispone ed effettua, tramite strumenti appositi ed in massima sicurezza, delle campagne di phishing simulate, verso gli utenti, atte ad aumentare l'attenzione richiesta ai punti precedenti. Tali campagne inviano finte email di phishing di vario tipo atte a verificare il comportamento degli utenti come ad esempio il clic su link, l'apertura di allegati o l'inserimento di credenziali che riproducono in tutta sicurezza potenziali casistiche malevoli. Lo strumento predisposto dal SIA tiene traccia delle eventuali azioni degli utenti che "cadono nei tranelli" invitandoli a seguire un breve webinar formativo di pochi minuti in merito alle azioni effettuate. Il webinar è da considerarsi come formazione obbligatoria.

12. Servizi e procedure di assistenza informatica

12.1 - Le procedure operative per le richieste di assistenza/servizi di cui al successivo punto 12.2) al servizio SIA, sono regolate da apposita procedura di apertura di ticket al portale web dedicato presente nella rete intranet dell'Unione:

https://pyunione.unionerenolavinosamoggia.bo.it/

Qualunque richiesta di assistenza informatica deve quindi essere segnalata tramite l'apertura di un ticket e **non sono modalità valide la telefonata, l'invio di una email o il raccolto de visu** a meno di casi particolari concordati con il Responsabile del servizio SIA. Sono caso particolari:

- servizi di sportello ai cittadini
- personale in servizio in sedi che non hanno l'accesso alla rete intranet dell'Unione

Poiché il portale di gestione delle richieste di assistenza è stato attivato in primo luogo a garanzia dei richiedenti che in tal modo possono monitorare lo stato dei propri ticket ed il periodo di giacenza degli stessi, oltre che per dotare i tecnici di un unico spazio in cui siano visibili e concentrate tutte le richieste aperte, **al di fuori dei casi particolari sopra indicati, una richiesta di assistenza informatica effettuata fuori del sistema di ticketing non verrà considerata né evasa dal personale tecnico del servizio SIA.**

Al fine di garantire una corretta e tempestiva assistenza, nel ticket si chiede di indicare necessariamente:

- ❏ un recapito telefonico diretto a cui essere contattati
- ❏ l'ubicazione della sede di lavoro (municipio, smart working etc)

12.2 - Il SIA tra le sue attività gestisce le principali richieste di assistenza/servizio, ovvero:

A. richiesta di acquisto, sostituzione di un PC, stampante, scanner e altre apparecchiature
B. richiesta di abilitazione all'accesso alla rete Internet
C. richiesta di abilitazione a specifici siti, servizi
D. richiesta di creazione del profilo di posta elettronica e abilitazione all'accesso della casella di posta elettronica e/o gruppi di servizio
E. richiesta di accesso alle informazioni presenti nelle cartelle condivise di servizio
F. richiesta di creazione, modifica e cancellazione di un'utenza per l'accesso ai servizi della rete comunale
G. richiesta di installazione di un nuovo applicativo
H. richiesta di abilitazione agli eventuali servizi erogati sulle Intranet per l'accesso a banche dati esterne (SIATEL, Servizi di Partout, e altri servizi on-line);
I. richiesta di abilitazione ai servizi erogati sulla Intranet comunale per l'accesso a banche dati interne (Anagrafe, Protocollo, ed altri servizi);
J. richiesta di ripristino del PC, stampante o altro dispositivo fornito dall'ente
K. richiesta di ripristino del funzionamento di software e programmi applicativi installati ed autorizzati
L. richiesta di dotare il personale di firma digitale (aperta dai responsabili di servizio) o di rinnovo della firma digitale

12.3 - Il personale tecnico del SIA effettua genericamente assistenza "da remoto" (senza recarsi in loco dall'utente) tramite software appositi di teleassistenza. La connessione ad un pc di un utente avviene sempre in accordo verbale con l'utente richiedente supporto e la procedura di connessione richiede, nel software di teleassistenza:

A. l'inserimento di una password da parte del tecnico del servizio SIA
B. l'approvazione esplicita da parte dell'utente

La presa in carico delle richieste di cui al punto 12.2) non è garantita qualora non venga rispettata la modalità descritta al punto 12.1). Salvo i casi indicati al punto 12.1), vengono considerate richieste "pendenti" solo quelle registrate tramite ticket nel portale delle richieste di assistenza.

12.4 - Il personale tecnico del SIA non è autorizzato ad effettuare alcuna assistenza né consulenza per quanto riguarda PC, device mobili o altre strumentazioni personali che non sono di proprietà dei Titolari.

13. Utilizzo delle stampanti e dei materiali di consumo

13.1 - 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 limitando le stampe ai soli casi in cui sia strettamente necessario per ragioni di lavoro. Ogni Dirigente/Responsabile di servizio è inviato a prendere contatti con il servizio SIA (per quanto di competenza) per lo studio di processi che siano finalizzati alla riduzione del consumo di carta.

14. Partecipazioni a social media

14.1 - L'utilizzo a fini promozionali e commerciali dei social media – quali Facebook™, Twitter™, Linkedin™, Instagram™, ecc, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dai Titolari attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti (conformemente a quanto disposto al precedente punto 10.2).

14.2 - Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, i Titolari ritengono comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio aziendale, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che viene vietata la partecipazione agli stessi social media durante l'orario di lavoro. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dal Titolare, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti degli stessi Titolari.

14.3 - La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dai Titolari riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sui piani industriali, sui clienti, sui fornitori ed altri partners dei Titolari stesso. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dei Titolari; l'utente, nelle proprie comunicazioni, non potrà quindi inserire marchi od altri segni distintivi del Titolare, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione Generale dei Titolari.

14.4 - L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso del Dirigente/Responsabile di servizio.

14.5 - L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso i Titolari, i colleghi, i clienti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito aziendale.

14.6 - Infine, in via generale ed ove non autorizzato in senso diverso dal proprio Dirigente/Responsabile di servizio, l'utente, nell'uso dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con i Titolari, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili ai Titolari.

15. Osservanza delle disposizioni in materia di Privacy

15.1 - È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati/soggetto terzo.

15.2 - Gli strumenti tecnologici considerati nel presente documento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970; conseguentemente, le informazioni raccolte sulla base di quanto qui indicato, anche conformemente al successivo paragrafo 16, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendo stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al successivo punto 17), fermo restando il rispetto della normativa in materia di protezione dei dati personali (GDPR 2016/679).

15.3 - **Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori**; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, il Titolare procederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970, dandone anche opportuna informazione agli utenti stessi.

16. Accesso ai dati trattati dall'utente

16.1 - Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale del servizio SIA o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure di cui ai precedenti punti 4.3) e 4.4), a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

17. Sistemi di controlli graduali

17.1 - In caso di anomalie, il personale incaricato del servizio SIA effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del servizio in cui è stata rilevata l'anomalia, nei quali si evidenzierá l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

17.2 - Per le finalità di cui al punto precedente, si comunica che i controlli ad oggi tecnologicamente possibili sono i seguenti:

a) controllo sui file di log prodotti da:
   - sistemi operativi
   - apparati di rete
   - software antivirus e sicurezza informatica
b) verifica attributi (tipologia, dimensioni etc) di file all'interno delle cartelle di rete e visualizzazione degli stessi

Da tali controlli è possibile reperire diverse informazioni sull'utilizzo da parte degli utenti delle dotazioni informatiche tra cui si evidenziano le principali:

- siti web visualizzati
- contenuti delle cartelle di rete
- stato di accensione dei pc anche fuori dell'orario di lavoro
- esecuzione di applicativi non consentiti

17.3 - In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

18. Modalità di lavoro, smart working e flessibile

18.1 Per i casi in cui l'attività lavorativa venga prestata in modalità di smart working o modalità flessibile, in merito alla strumentazione utile al dipendente per lo svolgimento dell'attività lavorativa, si specifica che:

- il pc deve essere aziendale e fornito dall'Ente. Non è consentito l'uso di dispositivi di pc di proprietà del dipendente.
- monitor, mouse e tastiera possono essere di proprietà del dipendente.
- non è consentita la connessione ai pc aziendali e quindi l'uso di supporti rimovibili personali o forniti da soggetti diversi dell'ente di appartenenza (es: chiavette USB) a cui si applicano tutte le disposizioni del paragrafo 8. L'Ente può fornire tali periferiche aziendali, previa verifica dell'effettiva necessità.
- non è consentita la connessione ai pc aziendali e quindi l'uso di stampanti e scanner di proprietà del dipendente.
- per i dispositivi mobili, telefoni smartphone e tablet, si rimanda a quanto indicato all' art. 7.2
- in generale non è consentita la connessione ai pc aziendali e quindi l'uso di altre categorie di strumentazione di proprietà del dipendente, non specificate nei punti precedenti.

18.2 - Per i casi in cui l'attività lavorativa venga prestata in modalità di smart working o in modalità flessibile, oltre a richiamare tutte le disposizioni elencate all'interno del presente documento, ad eccezione di quelle incompatibili con il presente articolo, si conferma la necessità di rispettare i seguenti principi funzionali all'osservanza ed alla corretta applicazione del Reg. UE 2016/679 (GDPR):personali

1. in presenza di problematiche tecniche o di sicurezza informatica che impediscano o ritardino sensibilmente lo svolgimento dell'attività lavorativa in smart working o in modalità flessibile, anche derivanti da rischi di perdita o divulgazione di informazioni dell'Ente, il dipendente sarà tenuto a dare tempestiva informazione al proprio responsabile (designato al trattamento).

2. fermo restando che la sede di lavoro resta invariata ad ogni effetto di legge e di contratto, in occasione della prestazione lavorativa effettuata in smart working o in modalità flessibile, il dipendente potrà effettuare la prestazione in altro luogo purché presso strutture o spazi riservati, riparati e protetti, secondo le indicazioni date in base alle linee guida per la protezione dei dati e la sicurezza. Il lavoratore è tenuto alla più assoluta riservatezza sui dati personali e sulle informazioni dell'Ente in suo possesso e/o disponibili sul sistema informatico dell'Ente che dovrà custodire con la massima cura, ed è altresì tenuto ad adottare tutte le precauzioni necessarie a garantire la salvaguardia e lo svolgimento delle attività in condizioni di sicurezza.

3. non è consigliabile portarsi della documentazione cartacea presso le proprie abitazioni, laddove ciò sia indispensabile, previa autorizzazione del designato o del titolare del trattamento (anche tramite email), potranno essere portati solamente le copie, non gli originali, dei documenti non contenenti dati particolari (sensibili) o documenti d'identità o informazioni strettamente personali e che rivelino situazioni di disagio.

4. il lavoratore è comunque tenuto a custodire con diligenza la documentazione, i dati e le informazioni dell'Ente utilizzati in connessione con la prestazione lavorativa, nonché al rispetto delle previsioni del Regolamento UE 679/2016 e del D.lgs. 196/2003 – così come novellato dal D.lgs 101/18 - in materia di privacy e protezione dei dati personali.

5. i dispositivi forniti dall'Ente non dovranno essere modificati nelle loro impostazioni di misure di sicurezza e di funzionamento.

19. Sanzioni

19.1 - È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente documento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, e nei confronti dei collaboratori, consulenti, agenti ed incaricati esterni di cui all'1.2, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.