

REGOLAMENTO INTERNO RELATIVO ALL'UTILIZZO DEI DATI

Vers. 2019/A

Regole di condotta ed obblighi dei collaboratori in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica redatto anche ai sensi del provvedimento del Garante della Privacy (Deliberazione n. 13 del 1/3/2007 - pubblicata sulla GU n. 58 del 10 marzo 2007) comprensivo di alcune note per la gestione dei dati cartacei.

Premessa

L'utilizzo di dispositivi informatici in azienda è sempre più diffuso e frequente. Questi ci consentono di velocizzare processi, comunicare all'interno e all'esterno dell'azienda, gestire attività e, in molti casi, sono indispensabili per fornire prodotti e servizi ai propri clienti. Computer, tablet e smartphone possono contenere tutto il know-how dell'azienda, dati sensibili, informazioni riservate. Ecco perché utilizzarli in modo sicuro e consapevole fa la differenza. È quindi fondamentale che i dipendenti conoscano regole, modalità d'uso, buone norme e divieti che consentano loro di agire sempre nel rispetto della privacy di clienti, colleghi, superiori, partner, e di tutte le figure che ruotano intorno all'azienda. La consegna del Regolamento interno relativo all'Utilizzo dei Dati agli incaricati (dipendenti o consulenti aziendali) costituisce una forma di tutela per l'Ente, titolare del trattamento dei dati, e fornisce gli strumenti idonei ad un corretto svolgimento delle mansioni da parte degli incaricati.

Il presente Regolamento Interno deve essere considerato una linea guida, uno spunto di riflessione per pensare a delle "Regole" aziendali ma, ovviamente, ogni organizzazione può personalizzarlo rendendolo il più aderente alla propria realtà, ma sempre nel rispetto della normativa privacy e dei Provvedimenti del Garante.

Il Regolamento Interno contiene i seguenti argomenti

1. SEZIONE I – AMBITO GENERALE

- 1.1. Definizioni
- 1.2. Premessa
- 1.3. Esclusione all'uso degli strumenti informatici
- 1.4. Titolarità dei device e dei dati
- 1.5. Finalità nell'utilizzo dei device
- 1.6. Restituzione dei device
- 1.7. Restituzione dei dati cartacei

2. SEZIONE II – PASSWORD

- 2.1. Le Password
- 2.2. Regole per la corretta gestione delle password
- 2.3. Divieto di uso
 - 2.3.1. Alcuni esempi di password non ammesse
- 2.4. La password nei sistemi
- 2.5. Audit delle password

3. SEZIONE III – OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

- 3.1. Login e Logout
- 3.2. Obblighi

4. SEZIONE IV - USO DEL PERSONAL COMPUTER DELL'ENTE

- 4.1. Modalità d'uso del COMPUTER aziendale
- 4.2. Corretto utilizzo del COMPUTER aziendale
- 4.3. Divieti Espressi sull'utilizzo del COMPUTER
- 4.4. ANTIVIRUS

5. SEZIONE V – INTERNET

- 5.1. Internet è uno strumento di lavoro
- 5.2. Misure preventive per ridurre navigazioni illecite
- 5.3. Divieti Espressi concernenti Internet
- 5.4. Divieti di Sabotaggio
- 5.5. Diritto d'autore

6. SEZIONE VI – POSTA ELETTRONICA

- 6.1. La Posta Elettronica è uno strumento di lavoro
- 6.2. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica
- 6.3. Divieti Espressi
- 6.4. Posta Elettronica in caso di assenze programmate ed assenze non programmate
- 6.5. Utilizzo Illecito di Posta Elettronica

7. SEZIONE VII – USO DI ALTRI DEVICE (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

- 7.1. L'utilizzo del notebook, tablet o smartphone
- 7.2. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ...)
- 7.3. Device personali.
- 7.4. Utilizzo del cellulare/smartphone personale.
- 7.5. Distruzione dei Device

8. SEZIONE VIII – SISTEMI IN CLOUD

- 8.1. Cloud Computing
- 8.2. Utilizzo di sistemi cloud

9. SEZIONE IX – GESTIONE DATI CARTACEI

- 9.1. Clear Desk Policy

10. SEZIONE X -APPLICAZIONE E CONTROLLO

- 10.1. Il controllo
- 10.2. Modalità di verifica
- 10.3. Modalità di Conservazione

11. SEZIONE XI – SOGGETTI PREPOSTI DEL TRATTAMENTO, INCARICATI E RESPONSABILI

- 11.1. Individuazione dei Soggetti autorizzati

12. SEZIONE XII – PROVVEDIMENTI DISCIPLINARI

- 12.1. Conseguenze delle infrazioni disciplinari
- 12.2 Diritti dell'interessato
- 12.2. Modalità di Esercizio dei diritti

13. SEZIONE XIII – VALIDITA', AGGIORNAMENTO ED AFFISSIONE , FIGURE DI RIFERIMENTO

- 13.1. Validità
- 13.2. Aggiornamento
- 13.3. Affissione DISCIPLINARE RELATIVO ALL'UTILIZZO DEI DATI
- 13.4 Figure di riferimento

1. SEZIONE I – AMBITO GENERALE

Ente : **A.S.P. DEL RUBICONE – Azienda Pubblica di Servizi Alla Persona**

D.Lgs. 196/2003: Decreto Legislativo 196 del 30 Giugno 2003 e sue successive modifiche ed integrazioni; integrato con le modifiche introdotte dal DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205)

NDA: non-disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.

Dipendente: personale dell'ente/organizzazione assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

Incaricato: ogni dipendente, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati personali

1.1. Definizioni

Si riportano qui di seguito le DEFINIZIONI riportate nell' Art. 4 del GDPR e art. 4 ex D.Lgs.196/2003

Azienda pubblica di Servizi alla Persona

A.S.P. DEL RUBICONE

Articolo 4

Definizioni

Ai fini del presente regolamento s'intende per:

- 1) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (C26, C27, C30)
- 2) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- 3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (C67)
- 4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (C24, C30, C71-C72)
- 5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (C26, C28-C29)
- 6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; (C15)
- 7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (C74)
- 8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- 9) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; (C31)
- 10) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- 11) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; (C32, C33)
- 12) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; (C85)
- 13) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; (C34)
- 14) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; (C51)
- 15) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (C35)

16) «**stabilimento principale**»: (C36, C37)

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale dell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento; (C80)

18) «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate; (C37, C48)

20) «**norme vincolanti d'impresa**»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune; (C37, C110)

21) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: (C124)

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

23) «**trattamento transfrontaliero**»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);

26) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

1.2. Premessa

L'ambito lavorativo porta il nostro Ente a gestire una serie di "informazioni", proprie e di terzi, per poter erogare i servizi che le vengono contrattualmente richiesti. Tali informazioni possono essere considerate, ai sensi del D.Lgs. 196/2003 e s.m.i., "dati personali" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'ente adotti una serie di misure minime ed idonee previste dalle norme.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'Ente è chiamato a garantire la riservatezza, o per NDA, o per una più ampia tutela del patrimonio aziendale.

Ai fini di questo Regolamento interno si specifica, pertanto, che con il termine "dati" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

Inoltre, nell'ambito della sua attività, l'ente tratta "dati cartacei" ovvero informazioni su supporto cartaceo e "dati digitali" ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'Ente stesso o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita dell'ente.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete internet dal computer aziendale espone l'ente a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'organizzazione stessa.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l'ente ha adottato il presente Regolamento interno diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Il presente Disciplinare Interno si applica agli **Incaricati** che si trovino ad operare con dati dell'ente.

Una gestione dei dati cartacei, un uso dei COMPUTER e di altri dispositivi elettronici (di seguito DEVICE) nonché dei servizi di internet e della posta elettronica difforme dalle regole contenute nel presente Regolamento interno potrebbe esporre l'organizzazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.

Le informazioni contenute nel presente Regolamento interno vengono rilasciate anche ai sensi dell'art. 13 del Codice sulla Privacy D.lgs 196/2003 e art. 13 del GDPR e costituiscono, quindi, parte integrante dell'informativa rilasciata agli Incaricati.

1.3. Esclusione all'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, l'ente/organizzazione valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari device aziendali, di internet e della posta elettronica da parte degli incaricati.

Successivamente e periodicamente l'ente/organizzazione valuta la permanenza dei presupposti per l'utilizzo dei device aziendali, di internet e della posta elettronica.

E' fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali.

I casi di esclusione possono riguardare:

1. L'utilizzo del COMPUTER o di altri DEVICE;
2. L'utilizzo della posta elettronica;
3. L'accesso a internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici nonché al principio di necessità di cui al Codice Privacy. Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo gli incaricati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.

I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi.

Si informa che tali esclusioni sono divenute necessarie alla luce del Provvedimento del Garante 1° marzo 2007 che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.

1.4. Titolarità dei device e dei dati

L'Ente è esclusivo titolare e proprietario dei Device messi a disposizione degli Incaricati ai soli fini dell'attività lavorativa.

L'ente è l'unico esclusiva titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri device digitali o archiviati in modo cartaceo nei propri locali.

L'incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei device aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'Ente.

Azienda pubblica di Servizi alla Persona

A.S.P. DEL RUBICONE

1.5 Finalità nell'utilizzo dei device

I device assegnati sono uno strumento lavorativo nelle disponibilità dell'Incaricato esclusivamente per un fine di carattere lavorativo. I device, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Regolamento interno.

Qualsiasi eventuale tolleranza da parte di questo ente/organizzazione, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Regolamento interno.

1.6. Restituzione dei device

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con l'Ente o, comunque, al venir meno, ad insindacabile giudizio dell'ente, della permanenza dei presupposti per l'utilizzo dei device aziendali, gli incaricati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei device in uso;
2. Divieto assoluto di formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

1.7. Restituzione dei dati cartacei

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con l'Ente o, comunque, al venir meno, ad insindacabile giudizio dell'ente, della permanenza dei presupposti per l'utilizzo di dati cartacei aziendali, gli incaricati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
2. Divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

2. SEZIONE II –PASSWORD

2.1. Le Password

Le password possono essere un metodo di autenticazione assegnato dall'organizzazione per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'ente nel suo complesso. Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza.

L'ente ha implementato alcuni meccanismi che permettono di aiutare e supportare gli Incaricati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso al Dominio (ove previsto), è in funzione un sistema automatico di richiesta di aggiornamento delle stesse impostato dall'ente secondo il livello di sicurezza richiesto dall'ente stesso e, comunque, in linea con quanto richiesto dalla normativa privacy.

Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone.

Le password che non vengono utilizzate da parte degli incaricati per un periodo superiore ai sei mesi verranno disattivate dall'ente.

In qualsiasi momento l'Ente si riserva il diritto di revocare all'Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

2.2. Regole per la corretta gestione delle password

L'Incaricato, da parte sua, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:

1. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. Occorre cambiare immediatamente una password non appena si abbia alcun dubbio che sia diventata poco "sicura";
3. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali e numeri;
4. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);

5. Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password.
6. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'ente.

Per caratteri speciali si intendono, per esempio, i seguenti: {} [], . < > ; : ! " £ \$ % & / () = ? ^ \ | ' * - + _.

In alcuni casi, sono implementati meccanismi che consentono all'Incaricato fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti. In caso di necessità contattare il Responsabile Esterno per L'assistenza e manutenzione del Parco Informatico.

2.3. Divieto di uso

Al fine di una corretta gestione delle password, l'organizzazione stabilisce il divieto di utilizzare come propria password:

1. Nome, cognome e loro parti;
2. Lo username assegnato;
3. Un indirizzo di posta elettronica (e-mail);
4. Parole comuni (in Inglese e in Italiano);
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. Parole banali e/o di facile intuizione, ad es. pippo, security e palindromi (simmetria: radar);
7. Ripetizioni di sequenze di caratteri (es. abcabcabc);
8. Una password già impiegata in precedenza.

2.3.1. Alcuni esempi di password non ammesse

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare. Alcuni esempi di password da evitare:

1. password = parte dell' user name o user name
2. Il nome della moglie/marito, fidanzato/a, figli, ecc.;
3. La propria data di nascita, quella del coniuge, ecc.;
4. Targa della propria auto;
5. Numero di telefono proprio, del coniuge, ecc.;
6. Parole comuni tipo "Password", "Qwerty", "12345678"

2.4. La password nei sistemi

Ogni Incaricato può variare la propria password di accesso a qualsiasi sistema aziendale in modo autonomo, qualora il sistema in questione metta a disposizione degli Utenti una funzionalità di questo tipo (Change password). La password può essere sostituita dal Referente Informatico Esterno (Responsabile dell'assistenza e manutenzione del parco informatico), anche qualora l'Utente l'abbia dimenticata.

2.5. Audit delle password

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, l'ente potrebbe effettuare analisi periodiche sulle password degli Incaricati al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente gli Incaricati stessi.

Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e all'Incaricato richiesto di cambiarla.

3. SEZIONE III –OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

In questa sezione vengono trattate le operazioni a carico dell'Incaricato e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

3.1. Login e Logout

Il "Login" è l'operazione con la quale l'Incaricato si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede un username e una password.

In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, l'Ente potrà assegnare un univoco user name e password per gruppi di incaricati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

3.2. Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L'incaricato deve quindi eseguire le operazioni seguenti:

1. Se si allontana dalla propria postazione dovrà mettere in protezione il suo device affinché persone non autorizzate non abbiano accesso ai dati protetti.
2. Bloccare il suo device prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
3. Chiudere la sessione (Logout) a fine giornata;
4. Spegner il PC dopo il Logout;
5. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo device.

4. SEZIONE IV -USO DEL PERSONAL COMPUTER DELL'ENTE

4.1. Modalità d'uso del COMPUTER aziendale

Il sistema informativo aziendale è composto da un insieme di unità server centrali e macchine client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi.

I files creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata sul sistema di repository documentale centralizzato. L'Ente non effettua il backup dei dati memorizzati in locale.

4.2. Corretto utilizzo del COMPUTER aziendale

Il computer consegnato all'incaricato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall'organizzazione. Per necessità aziendali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memoria di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto.

In particolare l'Incaricato deve adottare le seguenti misure:

1. Utilizzare solo ed esclusivamente le aree di memoria della rete dell'ente ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete;
2. Spegner il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché 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;
3. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall'organizzazione;

4. Non dare accesso al proprio computer ad altri utenti, a meno che siano incaricati con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

4.3. Divieti Espresi sull'utilizzo del COMPUTER

All'incaricato è vietato:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere.
2. Modificare le configurazioni già impostate sul personal computer.
3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'ente.
4. Installare alcun software di cui l'ente non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'organizzazione. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.
5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'organizzazione.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali per esempio virus, trojan horses ecc.
8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
9. Effettuare in proprio attività manutentive.
10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'organizzazione.

4.4. ANTIVIRUS

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail etc...

L'ente impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.

L'incaricato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

1. Comunicare all'ente ogni anomalia o malfunzionamento del sistema antivirus;
 2. Comunicare all'ente eventuali segnalazioni di presenza di virus o file sospetti.
- Inoltre, all'incaricato:
1. È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
 2. È vietato ostacolare l'azione dell'antivirus aziendale;
 3. È vietato disattivare l'antivirus senza l'autorizzazione espressa dell'ente anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer
 4. È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani.

Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

5. SEZIONE V –INTERNET

5.1. Internet è uno strumento di lavoro

La connessione alla rete internet dal device avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.

In particolare si vieta l'utilizzo dei social network, se non espressamente autorizzati.

5.2. Misure preventive per ridurre navigazioni illecite

L'organizzazione potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

5.3. Divieti Espresi concernenti Internet

1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare dati sensibili ai sensi del Codice Privacy.
 2. È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
 3. È vietato all'Incaricato lo scarico di software (anche gratuito) prelevato da siti Internet;
 4. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto.
 5. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
 6. È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'organizzazione, salvo specifica autorizzazione dell'organizzazione stessa.
 7. È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
 8. È vietato all'Incaricato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.
 9. È vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'ente stesso.
 10. È vietato, infine, creare siti web personali sui sistemi dell'organizzazione nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.
- Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è posta sotto la personale responsabilità dell'Incaricato inadempiente.

5.4. Divieti di Sabotaggio

È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'ente per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

5.5. Diritto d'autore

È vietato utilizzare l'accesso ad internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, ...) se non espressamente autorizzato dall'Ente.

6. SEZIONE VI –POSTA ELETTRONICA

6.1. La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente.

Gli Incaricati possono avere in utilizzo indirizzi nominativi di posta elettronica.

Le caselle e-mail possono meglio essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, direttore sanitario, consulenza, ...) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito.

Gli Incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

6.2. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

L'Ente è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli Incaricati e allo scopo prevede le seguenti misure:

1. In caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati.
2. Avvisare l'Ente quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

6.3. Divieti Espresi

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali.
2. È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti a destinatari esterni dell'organizzazione, senza utilizzare il seguente disclaimer:

Le informazioni contenute in questo messaggio sono riservate e confidenziali e il loro utilizzo è consentito esclusivamente al destinatario del messaggio, per le finalità indicate nello stesso. Qualora Lei non fosse la persona destinataria, La invitiamo ad eliminare il messaggio dal Suo Sistema ed a distruggere le varie copie o stampe, dandocene gentilmente comunicazione. Si prega di essere consapevoli che qualsiasi divulgazione, distribuzione o duplicazione è severamente vietato, e può essere illegale, e che ogni utilizzo improprio è contrario ai principi del REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO (Regolamento Generale sulla Protezione dei Dati). L'Azienda Pubblica di Servizi alla Persona "A.S.P. del Rubicone" ha fatto i possibili controlli per assicurarsi che questo messaggio ed eventuali allegati siano privi di Virus. Si consiglia comunque di trattare lo stesso applicando le corrette procedure per assicurarsi che ne sia privo al suo utilizzo.

The information contained in this message as well as the attached file(s) is confidential/privileged and is only intended for the person to whom it is addressed. If the reader of this message is not the intended recipient or the employee or agent responsible for delivering the message to the intended recipient, or you have received this communication in error, please be aware that any dissemination, distribution or duplication is strictly prohibited, and can be illegal. Any misuse is contrary to the principles of the REGULATION (EU) No 679/2016 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.(General Data Protection Regulation). Please notify us immediately and delete all copies from your mailbox and other archives. Although Azienda Pubblica di Servizi alla Persona "A.S.P. del Rubicone" have taken steps to insure that this e-mail and attachments are free from any virus, we advise that in keeping with good computing practice, the recipient should ensure they are actually virus free.

3. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.
4. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
5. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.

6.4. Posta Elettronica in caso di assenze programmate ed assenze non programmate

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (Auto-reply).

In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, l'Incaricato deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i files necessari a chi ne abbia urgenza.

Qualora l'Incaricato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irraggiungibile, l'Ente, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica dell'incaricato, informandone l'incaricato stesso e redigendo apposito verbale.

6.5. Utilizzo Illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'organizzazione.

7. SEZIONE VII –USO DI ALTRI DEVICE (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

7.1. L'utilizzo del notebook, tablet o smartphone.

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "device mobile") possono venire concessi in uso dall'organizzazione agli Incaricati che durante gli spostamenti necessitano di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'Ente.

L'Incaricato è responsabile dei device mobili assegnatigli dall'Ente e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai device mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i files creati o modificati sui device mobili devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai device mobili (Wiping).

Sui device mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'ente/organizzazione. I device mobili utilizzati all'esterno (convegni, visite in azienda, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei device mobili deve far seguito la denuncia alle autorità competenti.

Allo scopo si deve avvisare immediatamente l'ente che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche di giorno, durante l'orario di lavoro, all'Incaricato non è consentito lasciare incustoditi i device mobili.

All'Incaricato è vietato lasciare i device mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I device mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciati privi di PIN.

Laddove il device mobile sia accompagnato da un'utenza, l'Incaricato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, ...) e a rispettarli.

Qualora esigenze lavorative richiedessero requirements differenti l'Incaricato è tenuto ad informare tempestivamente e preventivamente l'ente/organizzazione.

In relazione alle utenze mobili, salvo autorizzazione dell'Ente, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'Ente, gli utilizzi all'estero devono essere preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

7.2. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)

Agli Incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, ...) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, ...).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

7.3. Device personali.

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, device personali.

Al dipendenti, se espressamente autorizzati dall'ente/organizzazione, è permesso solo l'utilizzo della posta elettronica aziendale sui loro device personali.

In tal caso è necessario che il device abbia password di sicurezza stringenti approvate dall'ente e l'eventuale furto o smarrimento del device deve essere immediatamente segnalato anche all'ente per eventuali provvedimenti di sicurezza.

Al collaboratore è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, ...).

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri device personali per memorizzare dati dell'ente solo se espressamente autorizzati dall'ente stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali device dovranno essere preventivamente valutati dall'ente, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

7.4. Utilizzo del cellulare/smartphone personale.

Durante l'orario di lavoro, comprese le eventuali pause, agli Incaricati è concesso l'utilizzo del telefono cellulare personale ma solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo.

In caso di trasferte lavorative all'esterno degli uffici dell'organizzazione, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l'organizzazione stessa ove fosse necessario.

In questo caso si invita, comunque, a non utilizzarlo per fini personali, in modo particolare alla presenza di clienti o fornitori.

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri cellulari/smartphone per memorizzare dati dell'ente solo se espressamente autorizzati dall'ente stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali cellulari/smartphone dovranno essere preventivamente valutati dall'ente, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

7.5. Distruzione dei Device

Ogni Device ed ogni memoria esterna affidati agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'ente che provvederà a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare l'ente provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

8. SEZIONE VIII –SISTEMI IN CLOUD

8.1. Cloud Computing

In informatica con il termine inglese cloud computing (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.

Le risorse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'utente, ma gli sono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'utente parte dell'onere della configurazione.

Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.

Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'ente/organizzazione a potenziali problemi di violazione della privacy.

I dati personali vengono memorizzati nelle server farms di aziende che spesso risiedono in uno stato diverso da quello dell'ente. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti,

Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'ente, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso da paese dell'utente.

Nel caso di industrie o aziende, tutti i dati memorizzati nelle memorie esterne sono seriamente esposti a eventuali casi di spionaggio industriale.

8.2. Utilizzo di sistemi cloud

E' vietato agli incaricati l'utilizzo di sistemi cloud non espressamente approvati dall'ente/organizzazione. Per essere approvati i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud esclusivi e non condivisi;
- Essere sistemi cloud posizionati fisicamente in Italia o nella Comunità Europea ;come previsto dal GDPR
- L'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile del Trattamento dei dati da parte dell'ente/organizzazione;
- L'azienda che fornisce il sistema in cloud deve comunicare all'ente/organizzazione, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati.
- Dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud.

9. SEZIONE IX –GESTIONE DATI CARTACEI

9.1. Clear Desk Policy

Gli Incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Gli Incaricati sono invitati dall'organizzazione ad adottare una "politica della scrivania pulita". Ovvero si richiede agli incaricati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'ente/organizzazione.

I principali benefici di una politica della scrivania pulita sono:

- 1) Una buona impressione a clienti e fornitori che visitano la nostra organizzazione;
- 2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
- 3) La riduzione che documenti confidenziali possano essere sottratti all'organizzazione.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassetiera, archivio, ...) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'ente.

A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.

Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archivarli digitalmente.

E' necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax o multifunzione, per evitare che siano prelevati o visionati da soggetti non autorizzati.

Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

10. SEZIONE X -APPLICAZIONE E CONTROLLO

10.1. Il controllo

L'ente, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
3. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assesment del sistema informatico.

Per tali controlli l'Ente si riserva di avvalersi di soggetti esterni.

Si precisa, in ogni caso, che l'Ente non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

10.2. Modalità di verifica

In applicazione del principio di necessità di cui all'art. 3 del Codice Privacy, l'Ee promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli Incaricati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

L'ente informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

10.3. Modalità di Conservazione

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

1. Ad esigenze tecniche o di sicurezza del tutto particolari;
2. All'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3. All'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

11. SEZIONE XI –SOGGETTI PREPOSTI DEL TRATTAMENTO, INCARICATI E RESPONSABILI

11.1. Individuazione dei Soggetti autorizzati

L'Ente ha designato ,con lettera di nomina di " **Incaricati del Trattamento dei dati Personali Comuni**" e " **Incaricati del Trattamento dei dati Personali Comuni e Particolari**" gli Incaricati.

Ha nominato i **Responsabili Esterni** , con "lettera di nomina di **Responsabili Esterni del Trattamento**", per le finalità riportate in ogni singola Lettera di Nomina , cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità.

Per quanto riguarda i soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) sono stati appositamente incaricati di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza realizzare attività di controllo a distanza, neanche di propria iniziativa.

I soggetti che operano quali amministratori di sistema o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, svolgono un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

12. SEZIONE XII –PROVVEDIMENTI DISCIPLINARI

12.1. Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Regolamento interno potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui:

1. Il biasimo inflitto verbalmente;
2. Lettera di richiamo inflitto per iscritto;
3. Multa;
4. La sospensione dalla retribuzione e dal servizio;
5. Il licenziamento disciplinare e con le altre conseguenze di ragioni e di legge;

Per i dirigenti valgono le vigenti norme di legge e/o di contrattazione collettiva, fermo restando che, per le violazioni di maggior gravità l'ente potrà procedere al licenziamento del dirigente autore dell'infrazione.

12.2. Diritti dell'interessato

Informiamo che gli artt. 11- 20 del Regolamento Europeo sulla Protezione dei Dati (GDPR) conferiscono agli interessati l'esercizio di specifici diritti. I diritti riconosciuti agli interessati ai sensi dell'art. 7 del Codice della Privacy restano invariati; con il Regolamento vengono aggiunti ad essi ulteriori diritti come il diritto ad ottenere dal titolare la conferma dell'esistenza o meno di propri dati personali e che tali dati vengano messi a disposizione in forma intellegibile; di conoscere l'origine dei dati nonché la logica e le finalità su cui si basa il trattamento; di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge nonché l'aggiornamento, la rettificazione o, se vi è interesse, l'integrazione dei dati; di opporsi, per motivi legittimi, al trattamento stesso. Il Regolamento Europeo riconosce, inoltre, all'interessato il diritto di presentare un reclamo all'autorità di controllo, il diritto di revocare il consenso in qualsiasi momento ed il diritto alla portabilità dei dati.

12.3. Modalità di Esercizio dei diritti

Per l'esercizio di tali diritti, l'interessato, potrà rivolgersi direttamente alla nostra Società **A.S.P. DEL RUBICONE - Via Manzoni n. 19 - 47030 San Mauro Pascoli (FC)**, contattabile telefonicamente allo **0541 933902** o all'indirizzo mail **segreteria@aspdelrubicone.it**.

L'interessato può inoltre proporre reclamo rivolgendosi al Garante per la protezione dei dati personali, consultando il sito web all'indirizzo <http://www.garanteprivacy.it/>. Si comunica che l'esercizio dei diritti dell'interessato di cui ai suddetti articoli, quali il diritto di cancellazione o opposizione, incontra i limiti imposti dalla normativa fiscale.

13. SEZIONE XIII –VALIDITA', AGGIORNAMENTO ED AFFISSIONE

Il presente Disciplinare ha validità a partire da: **2019**

13.2. Aggiornamento

Il presente Regolamento interno **Vers. 2019/A**, sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'Ente o in caso di mutazioni legislative.

Ogni variazione del presente Regolamento interno sarà comunicata agli incaricati.

13.3. Affissione

Il presente Regolamento interno verrà reso disponibile presso l'ufficio Amministrativo e/o pubblicato sulla intranet aziendale e/o affisso nella bacheca aziendale, ai sensi dell'art. 7 della legge 300/70 e del CCNL.

Azienda pubblica di Servizi alla Persona
A.S.P. DEL RUBICONE

13.4 **Figure di riferimento**

All' interno dell' ente/organizzazione sono state indicate quali figure di riferimento per approfondimenti e/o chiarimenti in merito ai punti sopra elencati le seguenti persone :

Consulente esterno con gli incarichi di :

Specialist Privacy e Privacy Manager :e DPO :

Sirotti Pietro

contattabile al seguente indirizzo mail

dpo@aspdelrubicone.it

gdpr@computerlandcesena.it

S. Mauro Pascoli,

2019

A.S.P. DEL RUBICONE

Il Legale Rappresentante