Allegato 1

REGOLAMENTO PER L'UTILIZZO DEL LAVORO AGILE PER IL PERSONALE DELL'AGENZIA PER I SERVIZI NEL SETTORE AGROALIMENTARE DELLE MARCHE

Art. 1
Premessa e riferimenti normativi

1. Il presente regolamento disciplina, l'applicazione del lavoro agile ordinario (di seguito anche smart working o SW) al personale dell'ASSAM definendone ambiti di attivazione, modalità di esecuzione e limiti di accesso, nel rispetto dei seguenti riferimenti normativi:
   - Legge 7 agosto 2015, n. 124 "Deleghe al Governo in materia di riorganizzazione delle Amministrazioni pubbliche" art. 14, come modificato dalla Legge n. 27/2020 art. 87-bis co. 5 e dalla Legge n. 77/2020 art. 263 co. 4-bis;
   - Legge 22 maggio 2017, n. 81 "Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato", Capo II "Lavoro Agile";
   - Decreto Legge 17 marzo 2020, n. 18, convertito con modificazioni in Legge n. 27/2020, art. 87;
   - Direttiva della Presidenza del Consiglio dei Ministri 4 maggio 2020, n. 3 "Modalità di svolgimento della prestazione lavorativa nell'evolversi della situazione epidemiologica da parte delle pubbliche amministrazioni";
   - Decreto Legge 19 maggio 2020, n. 34, convertito con modificazioni in Legge 77/2020, art. 263;
   - D.M. Ministro per la Pubblica Amministrazione del 19 ottobre 2020 "Misure per il lavoro agile nella pubblica amministrazione nel periodo emergenziale";
   - DGR n. 309 del 9 marzo 2020 (Misure urgenti per attivazione dello Smart Working in via straordinaria per far fronte all'emergenza COVID-19);
   - DPCM del 23 settembre 2021 (decreto rientro in presenza) in attuazione dell'art. 87 comma 1 del DL. n. 18 del 17 marzo 2020 convertito con modificazioni dalla legge 24 aprile 2020 n. 27;
   - DM dell'8 ottobre 2021 relativo alle "modalità organizzative per il rientro in presenza dei lavoratori delle PP.AA.";
   - Intesa sullo "Schema di Linee guida in materia di lavoro agile nelle amministrazioni pubbliche, ai sensi dell'articolo 1, comma 6, del decreto del Ministro per la pubblica amministrazione recante modalità organizzative per il rientro in presenza dei lavoratori delle pubbliche amministrazioni (16 dicembre 2021)";

Art. 2
Definizioni e finalità

1. Ai fini del presente regolamento si intende per "*Lavoro agile"* quanto già espressamente previsto dall'art.18 della L. 81/2017 e cioè una modalità flessibile di esecuzione del rapporto di lavoro connotata da un'organizzazione delle attività per cicli, fasi e obiettivi e dallo svolgimento di parte dell'attività all'esterno della sede lavorativa senza vincoli di spazio e di orario, entro i soli limiti di durata del tempo di lavoro giornaliero e settimanale derivanti dalla legge e dalla contrattazione collettiva.
2. Il lavoro agile risponde alle seguenti finalità:
   a) sperimentare ed introdurre nuove soluzioni organizzative che favoriscano lo sviluppo di una cultura

gestionale orientata al lavoro per obiettivi e risultati e, al tempo stesso, ad un incremento di produttività;

b) favorire un'organizzazione ispirata a principi di flessibilità, autonomia e responsabilità e fondata su legami di fiducia, nell'ottica del superamento della logica del mero controllo visivo;

c) favorire la digitalizzazione e la dematerializzazione delle attività, dei processi e dei procedimenti, garantendo comunque il miglior impatto per l'utenza in termini di accessibilità, anche da remoto, ai servizi erogati dall'ente;

d) rafforzare le misure di conciliazione dei tempi di vita - lavoro dei/delle dipendenti;

e) promuovere la mobilità sostenibile tramite la riduzione degli spostamenti casa - lavoro nell'ottica di una politica ambientale sensibile alla diminuzione del traffico urbano in termini di volumi e di percorrenze;

f) contribuire alla razionalizzazione nell'utilizzo degli spazi, delle sedi di lavoro e delle dotazioni tecnologiche realizzando economie di gestione.

Art. 3
Destinatari

1. Il lavoro agile si applica a tutto il personale Assam del comparto e della dirigenza che svolge la propria prestazione nell'ambito di un rapporto di lavoro subordinato a tempo indeterminato o determinato, pieno o parziale, nel rispetto del principio di non discriminazione.
2. Il personale regionale del comparto e della dirigenza assegnato funzionalmente all'Assam, in posizione di comando o distacco in entrata, effettua domanda sulla base del presente regolamento, in accordo con i dirigenti responsabili.
3. Il personale Assam in posizione di comando o distacco in uscita può svolgere la prestazione lavorativa in modalità agile secondo la disciplina organizzativa prevista nell'ente ove svolge concreto servizio.
4. Per il personale nuovo assunto a tempo indeterminato o determinato e/o a tempo parziale l'applicazione del lavoro agile va coordinata con l'esperienza lavorativa acquisita; il dirigente valuta se autorizzare la modalità di smart working prima del termine del periodo di prova previsto contrattualmente.

Art. 4
Criteri per l'applicazione e procedura di accesso

1. Il lavoro agile si realizza all'interno del rapporto di lavoro in corso, rimanendo invariata sia la struttura di assegnazione che la posizione giuridico-economica. Per accedere alla modalità di lavoro agile i/le dipendenti dichiarano:
   - di saper utilizzare i software gestionali in uso presso l'Assam, relativamente al proprio ambito lavorativo/settore di riferimento;
   - di conoscere le modalità operative del lavoro agile, come da documentazione reperibile sulla Point – servizi al dipendente, sezione Smart Working – Manuali e Linee guida;
   - di aver preso visione delle disposizioni normative in materia di salute e sicurezza sui luoghi di lavoro e policy per la sicurezza informatica che si allegano al presente Regolamento (Allegati all'Accordo individuale: "Tutela della Salute e della Sicurezza del personale in Lavoro Agile" e "Policy per la sicurezza informatica e per l'utilizzo degli strumenti informativi e telematici").
2. L'attivazione dello smart working ha carattere volontario. Il/La dipendente interessato, previo accordo con il/la dirigente e, se presente, la PO di riferimento, concordati i termini, le modalità di svolgimento, le attività ed i relativi risultati da raggiungere, presenta specifica richiesta compilando il modulo disponibile sulla

piattaforma Cohesion Work denominato SWORD_A "Accordo individuale di lavoro agile". Tale modulo viene trasmesso al/alla dirigente di assegnazione per la relativa autorizzazione. Ai fini della validità dell'Accordo individuale, la presentazione della domanda da parte del/della dipendente e la validazione da parte del/della dirigente costituiscono sottoscrizione.

3. L'Accordo individuale per la prestazione di lavoro agile del personale dirigente è autorizzato dal/dalla dirigente gerarchicamente sovraordinato, ed è adattato alle peculiarità delle figure dirigenziali.
4. Il/La responsabile nell'autorizzare lo svolgimento del lavoro agile, tiene conto dei seguenti requisiti:
   a) garantire l'invarianza dei servizi resi all'utenza;
   b) prevedere un'adeguata rotazione del personale autorizzato al lavoro agile, assicurando la prevalenza del lavoro in presenza di ciascuno;
   c) non avere lavoro arretrato accumulato, ancora da smaltire e, qualora ce ne sia, predisporre un idoneo e documentabile piano di smaltimento;
   d) tener conto della mappatura delle attività, pubblicata sul sito istituzionale ASSAM, che possono essere rese in modalità agile, fermo restando che sono comunque esclusi i lavori in turno e quelli che richiedono l'utilizzo costante di strumentazioni non remotizzabili.
5. Nel rispetto dell'art. 18 comma 3 bis della Legge n. 81/2017 e s.m.i., è riconosciuta priorità alle richieste di esecuzione del rapporto di lavoro in modalità agile formulate da:
   a) dipendenti genitori nei 3 anni successivi alla conclusione del periodo di congedo di maternità previsto dall'art. 16 del testo unico delle disposizioni legislative in materia di tutela e sostegno della maternità e della paternità, di cui al D.Lgs. n. 151/2000;
   b) dipendenti genitori con figli in condizione di disabilità ai sensi dell'art. 3 comma 3 della Legge n. 104/1992;
6. In considerazione della natura flessibile dello smart working, fermo restando il possesso dei requisiti di cui al punto 4, l'Amministrazione favorisce l'accesso al lavoro agile per i/le dipendenti che si trovano in condizioni di particolare necessità, da valutare a cura del/della dirigente responsabile, non coperte da altre misure.
   A titolo esemplificativo e non esaustivo, possono costituire condizioni di particolare necessità, ai sensi del comma precedente le seguenti circostanze:
   a) dipendenti con disabilità nelle condizioni di cui all'art. 3, comma 3, della legge 5 febbraio 1992, n. 104, oppure che abbiano un familiare in situazione di disabilità nelle medesime condizioni di cui al citato art. 3, comma 3;
   b) dipendenti in condizioni di fragilità secondo le indicazioni contenute nel decreto del Ministero della Salute del 4 febbraio 2022;
   c) dipendenti logisticamente assegnati, per l'esercizio della propria attività lavorativa in locali "affollati", cioè nei quali non è possibile rispettare le distanze indicate negli appositi decreti del datore di lavoro;
   d) dipendenti che abbiano sede di lavoro a più di 30 km dalla propria residenza;
   e) dipendenti con figli di età inferiore a 12 anni.

Art. 5
Trattamento giuridico ed economico

1. La modalità di lavoro agile non incide sulla natura giuridica del rapporto di lavoro subordinato in corso, che rimane regolato dalle norme legislative e dai contratti collettivi di lavoro nazionali e integrativi.
2. Il/La dipendente continua ad essere assegnato alla struttura di appartenenza e il suo passaggio al lavoro agile implica unicamente l'adozione di una diversa modalità di svolgimento della prestazione. Il/La

dipendente conserva pertanto, per quanto compatibili, gli stessi diritti e obblighi di cui era titolare quando svolgeva la propria attività in via continuativa nei locali dell'ente. L'ente garantisce le stesse opportunità rispetto alle progressioni di carriera, iniziative di socializzazione e di formazione previste per tutti i/le dipendenti che svolgono mansioni analoghe nelle sedi dell'ente.

3. È garantita parità di trattamento economico e normativo dei lavoratori che utilizzano l'istituto del lavoro agile, anche in riferimento alle indennità e al trattamento accessorio sulla base dei contratti nazionali e decentrati vigenti. Resta fermo quanto previsto dall'art. 8, comma 7.
4. Nelle giornate di lavoro agile il/la dipendente non ha diritto all'erogazione del buono pasto.

Art. 6
Accordo individuale di lavoro

1. L'accordo individuale di smart working di cui al precedente art. 4, comma 2, redatto per iscritto sulla base del modello di cui all'allegato A al presente Regolamento, consiste in un accordo tra le parti contenente le modalità e le condizioni di svolgimento del lavoro agile.
2. L'Accordo individuale di lavoro nello specifico prevede:

   a) le attività da espletare e risultati da conseguire in smart working, tenendo conto della mappatura delle attività di cui al precedente art. 4, comma 4, lett d), e/o del decreto annuale delle linee di attività redatto da ciascun responsabile di struttura dirigenziale;

   b) la strumentazione tecnologica necessaria allo svolgimento dell'attività lavorativa fuori dalla sede di lavoro;

   c) la decorrenza della modalità agile, che non può essere precedente alla data di autorizzazione da parte del/della dirigente;

   d) la durata dello stesso, determinato in un periodo di un anno con possibilità di rinnovo. In fase di prima applicazione, la scadenza è fissata per tutti al 31.12.2022;

   e) gli obblighi connessi all'espletamento dell'attività in modalità agile e le forme di esercizio del potere direttivo e di controllo del datore di lavoro sulla prestazione resa dal lavoratore all'esterno dei locali dell'ente, nel rispetto di quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300 e s.m.i.;

   f) le modalità di svolgimento della prestazione lavorativa fuori dalla sede abituale di lavoro, con indicazione delle giornate di lavoro da svolgere a distanza;

   g) le fasce di contattabilità e i tempi di disconnessione;

   h) i luoghi prevalenti (ma non esclusivi) per l'esecuzione della prestazione lavorativa fuori dai locali dell'ente;

   i) le modalità di recesso o cessazione ai sensi del successivo articolo 15.

   All'accordo individuale sono allegati, costituendone parte integrante:

   - l'informativa in materia di tutela della salute e sicurezza dei/delle dipendenti nei luoghi di lavoro (Allegato A1);
   - la policy per la sicurezza informatica e per l'utilizzo degli strumenti informativi e telematici della Giunta regionale che viene recepita per quanto applicabile all'ASSAM (Allegato A2) ;

3. Al fine di recepire eventuali modifiche in ordine al sistema di misurazione e valutazione della performance organizzativa e individuale e gli aggiornamenti periodici delle attività da prestare in lavoro agile mappate, l'accordo individuale può essere rinnovato/integrato per la parte concernente le attività e i risultati da raggiungere, attraverso la compilazione di apposito modulo di Cohesion Work denominato SWINT_A "Accordo integrativo SW". Tale modulo ripropone l'intero Accordo Individuale ed è modificabile esclusivamente per i campi relativi alle attività e ai risultati, nonché alla strumentazione informatica.

4. Qualora, in corso di vigenza dell'accordo, il/la dipendente cambi struttura di assegnazione giuridica o lavorativa, l'accordo in essere cessa e occorre procedere alla sottoscrizione di un nuovo Accordo Individuale; lo stesso vale anche nel caso di modifica del contratto di lavoro (trasformazione da full time a part-time o viceversa, da part-time orizzontale a part-time verticale, progressione di carriera, comandi parziali in entrata/in uscita). Non occorre invece procedere ad un nuovo accordo nel caso in cui cambi il/la dirigente responsabile, ma resti inalterata la struttura di assegnazione. L'accordo individuale rimane inalterato anche nel caso in cui intervengano modifiche agli obiettivi e/o alle attività previste dall' "*Accordo Individuale per la prestazione di lavoro agile*" ovvero vi sia una modifica alla strumentazione utilizzata dal personale dipendente in smart working; in questo caso il/la dipendente è tenuto unicamente alla compilazione del documento SWINT_A "Accordo integrativo attività Lavoro Agile" su Cohesionwork.

Art. 7
Luoghi di lavoro

1. Nelle giornate di smart working è responsabilità del/della dipendente individuare, oltre agli spazi dell'ente in sedi diverse dalla propria o per i quali siano stati sottoscritti dallo stesso appositi accordi per l'utilizzo di spazi di coworking, luoghi, anche esterni alle sedi ASSAM (tra cui la propria abitazione o il proprio domicilio), idonei per lo svolgimento dell'attività lavorativa che, tenuto conto delle mansioni svolte e secondo un criterio di ragionevolezza, rispondano ai requisiti di idoneità, sicurezza e riservatezza e quindi siano idonei all'uso abituale di supporti informatici, non mettano a rischio l'incolumità del collaboratore, né la riservatezza delle informazioni e dei dati trattati nell'espletamento delle proprie mansioni e rispondano ai parametri di sicurezza sul lavoro indicati dall'ente.
2. Gli spazi predisposti dall'ente (es. sedi decentrate) o individuati da altri enti (es. sedi regionali) sono sempre da considerarsi idonei ed oggetto di verifiche di routine da parte degli uffici competenti.

Art. 8
Modalità di esecuzione della prestazione e orario di lavoro

1. L'attuazione dello smart working non modifica la regolamentazione dell'orario di lavoro applicata al/alla dipendente, che farà riferimento al "normale orario di lavoro" (full-time o part-time) con le caratteristiche di flessibilità temporali proprie dello smart working nel rispetto, comunque, dei limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione.
2. Nell'ambito dello svolgimento della prestazione lavorativa possono essere individuate 2 giornate la settimana, per un massimo di 8 giornate mensili - indipendentemente dal numero di settimane nel mese - in cui l'attività può essere resa in modalità smart working, assicurando pertanto la prevalenza del lavoro in presenza; in caso di rapporto di lavoro a tempo parziale verticale e comando/distacchi parziale, le giornate vengono riproporzionate. Resta garantita l'ampia flessibilità basata su un rapporto consapevole e di fiducia tra le parti e la possibilità di variare – anche temporaneamente e senza necessità di modifica formale dell'accordo - l'articolazione delle giornate sulla base di esigenze organizzative e/o personali.
3. In tal senso la variazione viene concordata con il/la dirigente, e l'eventuale Posizione Organizzativa di riferimento, e giustificata tramite specifico giustificativo SWCT_A "Cambio turno SW" di Cohesion Work, entro le 24 ore antecedenti, all'interno del mese in corso; in ogni caso i giorni di SW non fruiti nel mese non sono recuperabili nel mese successivo.
4. Ai fini della verifica del rispetto dell'orario di lavoro, la giornata di lavoro agile è considerata equivalente a quella svolta presso la sede di servizio.

5. Nelle giornate di lavoro agile il/la dipendente organizza autonomamente la prestazione lavorativa con riferimento al proprio orario teorico giornaliero e agli obiettivi assegnati nella fascia oraria standard 7.30 – 19,30. Al fine di garantire un'efficace interazione con la struttura di appartenenza ed uno svolgimento ottimale della prestazione lavorativa, il/la dipendente deve concordare una o più fasce orarie di contattabilità per un totale di 4 ore giornaliere, da specificare nell'accordo individuale (es. unica fascia di contattabilità ore 9,00 – 13,00 oppure 2 fasce di contattabilità 9,00-11,00 e 14,00 – 16,00 , ecc.). Rimane fermo il principio della disponibilità concordata preventivamente per le attività da svolgere collettivamente e il principio del rispetto delle tradizionali fasce di pausa, in particolare quella per il pranzo, nella programmazione di attività in forma collettiva.

   Al/alla dipendente è riconosciuto un periodo temporale di disconnessione dalle 19,30 alle 7,30, in cui non può erogare alcuna prestazione lavorativa, né può essere contattato telefonicamente, o via mail o con altre modalità similari.
6. Nelle fasce di contattabilità in caso di impossibilità da parte del lavoratore a rendersi reperibile, lo stesso deve darne tempestiva e motivata comunicazione al proprio responsabile e può richiedere, ove ne ricorrano i relativi presupposti, la fruizione dei permessi previsti dal CCNL o dalle norme di legge quali, a titolo esemplificativo, i permessi per particolari motivi personali o familiari, i permessi sindacali di cui al CCNQ 4 dicembre 2017 e s.m.i., i permessi di cui all'art. 33 della legge 104/1992.
7. Nelle giornate in cui la prestazione lavorativa viene svolta in modalità agile non è possibile effettuare lavoro straordinario, trasferte, lavoro disagiato, lavoro svolto in condizioni di rischio.
8. In caso di problematiche di natura tecnica e/o informatica, e comunque in ogni caso di cattivo funzionamento dei sistemi informatici, qualora lo svolgimento dell'attività lavorativa a distanza sia impedito, reso non sicuro o sensibilmente rallentato, il/la dipendente è tenuto a darne tempestiva informazione al proprio dirigente. Lo stesso può richiamare il/la dipendente a lavorare in presenza. In caso di ripresa del lavoro in presenza, si applica la disciplina di cui ai successivi commi 9 e 10.
9. Per sopravvenute e documentate esigenze di servizio il/la dirigente può richiamare in sede il/la dipendente, dandone comunicazione in tempo utile e comunque con un preavviso di almeno 24 ore; in tale ipotesi il/la dipendente effettua il giustificavo di cambio turno di cui al precedente comma 3 a condizione che la giornata di SW scelta in sostituzione dell'originale ricada nel mese in corso.
10. Nei casi eccezionali in cui si renda necessario il rientro in sede per motivi di servizio, ma non sia possibile rispettare il preavviso di 24 ore, il/la dipendente accede alla sede di lavoro previa timbratura. Il/La dipendente può completare l'orario di lavoro in sede e compilare un giustificativo di Cambio turno SW. In questo caso si applica la disciplina relativa al lavoro svolto presso la sede di lavoro. In alternativa, il/la dipendente può decidere di non completare l'orario in presenza e proseguire la giornata in SW come da calendario. In questo caso, le timbrature rilevano ai soli fini della sicurezza.
11. Non sarà consentita attività in lavoro agile in coincidenza delle giornate di chiusura di tutti i servizi e strutture nei presidi territoriali dell'ASSAM, come programmate e comunicate annualmente dall'ente.
12. Al fine di garantire il rispetto del limite di 8 giornate di lavoro agile nel mese, viene effettuato a inizio mese un controllo automatico del calendario delle giornate di sw indicate dal lavoratore, a seguito del quale lo stesso viene avvisato con specifica mail qualora dovessero esserci in quel mese più di 8 giorni di calendario teoricamente lavorabili in modalità agile. In tal caso, il lavoratore deve fare attenzione a rientrare in sede per evitare assenze ingiustificate.
13. Resta inteso che il giustificativo Cohesion denominato "Cambio turno – cod. A002" (cambio rientro) può essere utilizzato unicamente per le giornate di lavoro in sede.

Art. 9
Dotazione Tecnologica e Sicurezza dei dati

1. L'ente mette di norma a disposizione l'attrezzatura tecnologica adatta e necessaria per lo svolgimento della prestazione lavorativa in lavoro agile, sulla base di specifiche mansioni da svolgere.
   Qualora la strumentazione idonea da fornire, o parte di essa, non sia disponibile, il/la dipendente espleta la propria prestazione lavorativa in modalità agile avvalendosi di supporti informatici e connessione internet di sua proprietà o nella sua disponibilità; in tal caso viene garantita la verifica, da parte del referente informatico di riferimento, della configurazione delle impostazioni che eventualmente impediscono il corretto utilizzo dei sistemi informativi messi a disposizione dall'ente. Nel caso in cui più dipendenti richiedano strumentazione in numero eccedente le disponibilità dell'ente, nel definire le priorità si terranno in considerazione le effettive necessità documentate.
2. L'assetto standard della dotazione per lo smart working è il seguente:
   - un pc portatile comprensivo degli applicativi software utilizzati;
   - mouse
   - cuffie con microfono integrato;
   - docking station presso la sede Assam comprensiva di monitor e tastiera in sostituzione dell'attuale postazione fissa in ufficio;

   La connessione internet viene fornita a chi dichiari di esserne sprovvisto nel luogo o nei luoghi prevalenti di svolgimento dello smart working.
3. Il personale si impegna a custodire con la massima cura e mantenere integra la strumentazione che viene fornita, in modo tale da evitarne il danneggiamento, lo smarrimento ed a utilizzarla in conformità con le istruzioni ricevute (Allegato A2 "Policy per la sicurezza informatica e per l'utilizzo degli strumenti informativi e telematici").
4. L'accesso alle risorse digitali e alle applicazioni raggiungibili tramite la rete internet avviene attraverso il sistema di gestione di identità digitale "Cohesion" in grado di assicurare un livello di sicurezza adeguato. Qualora, si renda necessario accedere ai server contenenti applicativi, database o sistemi non fruibili tramite browser, l'Assam autorizza l'accesso alle risorse attraverso VPN (Virtual Private Network), previa verifica da parte del/della dirigente e del referente informatico e relativa comunicazione alla struttura competente in materia di sistemi informatici.
5. I costi sostenuti dal/dalla dipendente direttamente e/o indirettamente collegati allo svolgimento della prestazione lavorativa o le eventuali spese per il mantenimento in efficienza dell'ambiente di lavoro agile non sono a carico dell'ente.
6. Eventuali impedimenti tecnici (come malfunzionamenti della linea dati o problemi di comunicazione telefonica) allo svolgimento dell'attività lavorativa nelle giornate di lavoro agile devono essere tempestivamente comunicati dal/dalla dipendente al/alla dirigente e al proprio referente informatico al fine di dare rapida soluzione al problema. Qualora ciò non sia possibile, vanno concordate con il/la dirigente responsabile le modalità di completamento della prestazione, ivi compreso, ove possibile, il rientro del/della dipendente nella sede di lavoro, alle condizioni di cui al precedente art. 8 comma 8.
7. Alla postazione di lavoro agile sono applicati i normali protocolli di sicurezza previsti nell'ambito dei piani per il trattamento dei dati e per la salvaguardia della loro integrità e riservatezza, nel rispetto di standard di sicurezza equivalenti a quelli garantiti alle postazioni lavorative presenti negli uffici dell'ente. Il /La

dipendente in lavoro agile è tenuto al rispetto della normativa inerente il segreto d'ufficio e della normativa inerente la protezione dei dati personali di cui al D.Lgs. n. 196 del 2003 e al Reg.UE n. 679/2016, nonché a quanto stabilito nell'allegato A2 al presente Regolamento.

Art. 10
Formazione

1. Per agevolare ed ottimizzare l'utilizzo del lavoro agile, l'ente promuove la partecipazione a percorsi formativi in materia di: modalità operative dello smart working, utilizzo delle piattaforme di comunicazione, utilizzo dei principali applicativi gestionali dell'Ente, e quant'altro si renda necessario al fine di incentivare l'innovazione organizzativa e la modernizzazione dei processi di lavoro richiesti dal lavoro agile.
2. L'Ente garantisce ai/alle dipendenti che svolgono il lavoro in modalità agile le stesse opportunità formative, finalizzate al mantenimento e allo sviluppo della professionalità, previste per tutto il personale che svolge mansioni analoghe.

Art. 11
Sicurezza sul lavoro

1. Il/La dipendente che svolge la propria prestazione lavorativa in modalità smart working, sulla base della formazione ricevuta, nel rispetto dei requisiti di cui al presente regolamento - informativa Allegato A1 - è tenuto a rispettare ed applicare correttamente le direttive dell'ente e deve prendersi cura della propria salute e sicurezza, in linea con le disposizioni dell'art. 20 del D.lgs. 81/08, comma 1.
2. L'ente, ai sensi dell'art. 22, comma 1 della Legge n. 81/2017, garantisce la salute e la sicurezza del lavoratore che svolge la prestazione n modalità di lavoro agile.

Art. 12
Controlli e sanzioni

3. Nel caso di mancato rispetto delle regole previste nell'esercizio dell'attività lavorativa, incluse quelle previste per l'utilizzo della strumentazione informatica, di quelle inerenti al codice di comportamento applicabile al personale dell'ASSAM, verranno applicate le sanzioni indicate nel codice disciplinare vigente.

Art. 13
Assicurazione obbligatoria per gli infortuni e le malattie professionali

1. Il lavoratore ha diritto alla tutela contro le malattie professionali e gli infortuni sul lavoro dipendenti da rischi connessi alla prestazione lavorativa resa all'esterno dei locali. In ossequio a quanto stabilito dalla legge 22 maggio 2017, n. 81 ed in conformità alla circolare INAIL n. 48 del 2 novembre 2017, la tutela viene garantita anche per malattie e infortuni occorsi durante il percorso di andata e ritorno tra l'abitazione e il prescelto luogo di lavoro, quando la scelta del luogo della prestazione sia dettata da esigenze connesse alla prestazione stessa o dalla necessità del lavoratore di conciliare le esigenze di vita con quelle lavorative e risponda a criteri di ragionevolezza.

Art. 14
Valutazione e monitoraggio

1. L'attività svolta in modalità di agile e i risultati raggiunti, analogamente a quanto previsto per l'attività

lavorativa prestata in sede, sono oggetto di valutazione nell'ambito del sistema di misurazione e valutazione della performance organizzativa e individuale vigente nell'ente.

2. I/Le dirigenti monitorano con cadenza mensile, attraverso i report anche in formato digitale messi a disposizione dell'ente, in modo mirato e costante, l'attività prestata dal dipendente e il raggiungimento dei risultati attesi, anche confrontandosi con il dipendente stesso per condividere punti di forza e di debolezza e risolvere eventuali problematiche.
3. L'ente effettua con periodicità almeno annuale un monitoraggio del lavoro agile per indagare in merito agli impatti dello stesso sia sulla vita lavorativa e privata dei/delle dipendenti che sull'efficienza ed efficacia dell'attività dell'Assam.

Art. 15
Recesso

1. Durante lo svolgimento del lavoro agile, sia l'ente (in persona del/della dirigente di assegnazione per il personale del comparto e del dirigente sovraordinato individuato ai sensi della L.R. 30 luglio 2021 n.18 per il personale dirigenziale) sia il/la dipendente possono, fornendo specifica motivazione, recedere dall'accordo individuale prima della sua naturale scadenza, con un preavviso di 30 giorni, elevato a 90 nel caso di dipendenti con disabilità, salvo giustificato motivo. E' possibile la rinuncia al preavviso da parte del soggetto che subisce il recesso.
2. In particolare, costituisce giustificato motivo che autorizza il recesso dell'ente senza obbligo di preavviso il ricorrere delle seguenti circostanze:

a) l'efficienza e l'efficacia delle attività svolte dal/dalla dipendente non sono rispondenti ai parametri stabiliti;
b) sopravvenute esigenze di servizio non procrastinabili;
c) la mancata osservanza delle disposizioni in materia di salute e sicurezza sul lavoro, sicurezza e tutela dei dati, fedeltà e riservatezza.

3. L'Accordo perde automaticamente efficacia nel caso in cui cambino la struttura di assegnazione giuridica o lavorativa del/della dipendente, o la tipologia del contratto di lavoro, come già stabilito al precedente articolo 6, comma 4.

Art. 16 Disposizioni finali

1. Per tutto quanto non previsto dal presente Regolamento, si fa rinvio alle disposizioni che regolano gli istituti che disciplinano il rapporto di lavoro dei/delle dipendenti dell'Assam.
2. In caso di entrata in vigore di disposizioni contrattuali nazionali, decentrate e discipline regolamentari che apportino modifiche ad istituti applicati ai lavoratori con accordo di smart working, le norme di cui al presente Regolamento sono immediatamente modificate e/o disapplicate di conseguenza.
3. Resta salva la possibilità di modificare il presente Regolamento per rispondere ad eventuali esigenze emerse durante l'applicazione dello stesso, previo confronto con le organizzazioni sindacali maggiormente rappresentative.

Monica
Carteletti
31.03.2022
10:37:19
GMT+01:00

Allegato A

ACCORDO INDIVIDUALE PER LA PRESTAZIONE DI LAVORO AGILE
PERSONALE ASSAM

Si procede alla stipula dell'Accordo Individuale di lavoro agile *ex art. 6 Regolamento SW ASSAM*

TRA

(Nome e Cognome)_____direttore/dirigente della struttura_____ _____nato a_____il_____residente a _____, C.F._____

E

Il/la dipendente_____, nato/a a_____il_____ residente a_____C.F._____in servizio presso l'Agenzia per i Servizi nel Settore Agroalimentare delle Marche ASSAM, con tipologia di contratto (t.ind/t.det full time o p.time)_____categoria_____, profilo professionale_____

Visto il Decreto del Direttore di approvazione del Regolamento per la disciplina del lavoro agile per il personale dell'Agenzia per i Servizi nel Settore Agroalimentare delle Marche

si conviene quanto segue:

la/il dipendente è ammessa/o a svolgere la prestazione lavorativa in modalità agile, fuori dalla sede abituale di lavoro, nei termini e alle condizioni di seguito indicate e in conformità alle prescrizioni stabilite nel Regolamento sopra richiamato.

1) **Decorrenza e durata** *(indicare un periodo massimo di un anno)*

data di avvio prestazione lavoro agile: _____
(in ogni caso condizione per l'avvio è l'autorizzazione da parte del dirigente/direttore)

data di fine prestazione lavoro agile: _____

periodicità della prestazione di lavoro agile***(indicare quante e quali giornate all'interno della settimana saranno prestate in modalità agile, assicurando la prevalenza del lavoro in presenza):____*

*****per dipendenti con contratto full time è possibile indicare 2 giornate settimanili per un massimo di 8 giornate al mese; in caso di p.time verticale e comando/distacco parziale le giornate massime lavorabili in SW sono riproporzionate)*

2) **Fasce di contattabilità e tempi di disconnessione**

nel caso di un'unica fascia di contattabilità
dalle_____alle_____

nel caso di due fasce di contattabilità (*compilare)*

dalle_____alle_____

dalle_____alle_____

La fascia di disconnessione è dalle 19.30 alle 7.30

3) Strumentazione tecnologica necessaria allo svolgimento dell'attività

ai fini dello svolgimento dell'attività lavorativa in modalità agile, si prevede l'utilizzo della seguente dotazione tecnologica*:

a) fornita dall'ente:
   - □ *un pc portatile comprensivo degli applicativi software utilizzati;*
   - □ *mouse;*
   - □ *cuffie con microfono integrato;*
   - □ *connessione internet (nel caso di indisponibilità nei luoghi prevalenti);*
   - □ *altro (specificare)*_____

o, in alternativa

b) di proprietà/in utilizzo del/della dipendente:
   - □ *pc*
   - □ *cuffie con microfono*
   - □ *mouse*
   - □ *connessione internet*
   - □ *altro (specificare)*_____

**se la strumentazione è in parte fornita dall'ente, in parte di proprietà/in utilizzo del dipendente compilare entrambe le sezioni*

4) Luoghi prevalenti (ma non esclusivi) per lo svolgimento della prestazione (indicare i luoghi)

- ……..
- ……..
- ……..
- ……..

5) Obblighi connessi all'espletamento dell'attività in modalità agile

Il lavoratore si obbliga a non svolgere attività incompatibili con l'oggetto della prestazione lavorativa.
In caso di apparecchiature fornite dall'ente, il/la dipendente deve aver cura delle stesse e deve utilizzare gli strumenti tecnologici assegnati ed i software che vengano messi a sua disposizione dall'ente per l'esercizio esclusivo dell'attività lavorativa, nel rispetto delle disposizioni adottate in merito all'utilizzo degli strumenti e dei sistemi.
Durante lo svolgimento della prestazione lavorativa il/la lavoratore/lavoratrice si impegna a tenere un comportamento improntato a principi di correttezza e buona fede e a rispettare le disposizioni contenute nel Codice di comportamento e nel Codice disciplinare regionale applicato all'Assam.

6) Poteri del datore di lavoro

La prestazione lavorativa in modalità agile non modifica il potere direttivo e di controllo del

dirigente/direttore e se presente della PO di assegnazione, che viene esercitato con modalità analoghe a quelle applicate con riferimento alla prestazione resa presso i locali dell'ente.
Nell'ambito dei suoi poteri il/la dirigente/direttore/PO impartisce le precise istruzioni per la concreta esecuzione del lavoro agile e verifica che il/la dipendente si attenga alle istruzioni impartite, in particolare:

- identifica le attività da svolgere in modalità agile;
- definisce, condividendoli con il dipendente, gli obiettivi/ risultati da raggiungere ed eventuali priorità da seguire;
- monitorare e valuta i risultati conseguiti dal dipendente.

7) Recesso

1. Durante lo svolgimento del lavoro agile, sia l'ente in persona del dirigente/direttore di assegnazione, sia il/la dipendente possono, fornendo specifica motivazione, recedere dall'accordo individuale prima della sua naturale scadenza, con un preavviso di 30 giorni, elevato a 90 nel caso di dipendenti con disabilità, salvo giustificato motivo. E' possibile la rinuncia al preavviso da parte del soggetto che subisce il recesso.
2. In particolare, costituisce giustificato motivo che autorizza il recesso dell'amministrazione senza obbligo di preavviso il ricorrere delle seguenti circostanze:

a. l'efficienza e l'efficacia delle attività svolte dal dipendente non sono rispondenti ai parametri stabiliti;
b. sopravvenute esigenze di servizio non procrastinabili;
c. la mancata osservanza delle disposizioni in materia di salute e sicurezza sul lavoro, sicurezza e tutela dei dati, fedeltà e riservatezza.
3. L'Accordo perde automaticamente efficacia nel caso in cui cambino la struttura di assegnazione giuridica o lavorativa del dipendente, o la tipologia del contratto di lavoro, come stabilito dal Regolamento all' articolo 6, comma 4.

si stabilisce altresì:

a) **Attività da svolgere** (*elencare/descrivere le attività da espletare rinvenibili sul documento mappatura delle attività e/o decreto annuale delle linee attività della struttura):*

b) **Risultati da raggiungere** *(Indicare i principali risultati da raggiungere attraverso lo svolgimento delle attività sopraindicate):*

La/Il dipendente inoltre dichiara,

□ di saper utilizzare i software gestionali in uso nell'Agenzia, relativamente al proprio ambito lavorativo/settore di riferimento;
□ di conoscere le modalità operative del lavoro agile, come da documentazione reperibile sulla Point – servizi

al dipendente, sezione Smart Working – Manuali e Linee guida;

- □ di aver preso visione delle previsioni normative in materia di salute e sicurezza sui luoghi di lavoro e policy per la sicurezza informatica e di rispettare quanto previsto nell'informativa in materia di tutela della "Salute e della Sicurezza del personale in Lavoro Agile" (Allegato A1) e in materia di "Policy per la sicurezza informatica e per l'utilizzo degli strumenti informativi e telematici" (Allegato A2).

Per quanto non espressamente previsto nel presente accordo si rinvia al Regolamento per la disciplina del lavoro agile (smart working), adottato dall'ASSAM.

Id ……

La presentazione della domanda da parte del dipendente e la validazione del dirigente costituiscono sottoscrizione del presente Accordo individuale

Allegato A1

Allegato all'Accordo individuale di Lavoro Agile

INFORMATIVA
Tutela della Salute e della Sicurezza del personale in Lavoro agile
(art. 22 comma 1 Legge 81/2017)

1. PREMESSA

Il presente documento mira a fornire ai/alle lavoratori/trici agili (o *smart workers*) indicazioni utili in relazione alla tutela della salute e sicurezza, durante l'esecuzione della prestazione lavorativa in modalità di Lavoro agile ovvero all'esterno dei locali aziendali.
Tale modalità di prestare la propria attività lavorativa si distingue dal "telelavoro" per la flessibilità nella individuazione delle giornate da dedicare a questo tipo di svolgimento del lavoro e nella scelta del luogo ove prestare l'attività lavorativa, che non coincide necessariamente con il proprio domicilio. In virtù di ciò, il/la lavoratore/trice agile è tenuto a cooperare all'attuazione delle misure di prevenzione predisposte dal Datore di Lavoro per fronteggiare i rischi connessi all'esecuzione della prestazione all'esterno dei locali aziendali" (art. 22, comma 2, Legge 81/2017).
È dunque dovere del/della lavoratore/trice agile mettere in atto ogni comportamento utile a limitare i rischi derivanti dall'esecuzione della prestazione lavorativa al di fuori dei locali aziendali, dove viene meno la possibilità da parte del Datore di Lavoro di verifica puntuale del rispetto dei principi ergonomici e tecnici di salute e sicurezza sul lavoro. Più in generale si può dire che il/la lavoratore/trice agile:

- non dovrà in alcun modo adottare comportamenti che possano generare rischi per la sua salute e sicurezza o per quella di terzi;
- dovrà evitare ogni luogo, ambiente, situazione e circostanza che possa comportare un pericolo per la sua salute e la sua sicurezza o per quella di terzi.

2. PRINCIPI GENERALI

I luoghi di lavoro individuati per l'esecuzione della prestazione lavorativa in Lavoro agile devono rispettare, per quanto possibile, le indicazioni previste per la sicurezza dei videoterminalisti.
Il/la lavoratore/trice agile deve dunque rifarsi a quelle indicazioni per ciò che riguarda:

- i requisiti generali dei luoghi di lavoro;
- le caratteristiche della postazione di lavoro;
- le pause da rispettare;
- la corretta postura da tenere.

Di seguito vengono riepilogate tali indicazioni.

MICROCLIMA

Nei luoghi di lavoro devono essere garantite adeguate condizioni di salute e di benessere relativamente alla temperatura a cui si è esposti e alla qualità dell'aria, sia ricorrendo a scambi naturali con l'ambiente esterno sia utilizzando appositi impianti di riscaldamento e condizionamento dell'aria. Fermo restando che sono numerosi i fattori che influiscono sul microclima, non ultimi ad esempio il tipo di attività fisica svolta e l'abbigliamento indossato, di seguito sono indicate le condizioni per lavorare in un ambiente dal punto di vista microclimatico ottimale:

- è preferibile operare in un ambiente di lavoro con temperatura invernale oscillante tra i 18 °C e i 22 °C;
- è preferibile una differenza di temperatura interna estiva inferiore all'esterna di non più di 7 °C;
- per le attività svolte all'esterno è raccomandabile, ove possibile, evitare le ore della giornata in cui gli UV sono più intensi (ore 11,00 – 15,00 oppure 12,00 – 16,00 con l'ora legale).

I lavoratori che si trovano a operare in postazioni o in ambienti che, a loro giudizio, non offrono adeguate condizioni in termini di temperatura, livello di umidità o presenza di fastidiose correnti d'aria, devono ricercare le soluzioni che gli consentano il migliore comfort termico.

RISCHIO RUMORE

Le principali cause di rumorosità sono identificabili:

- nell'eccessivo affollamento;
- nel sovrapporsi di conversazioni ad elevato volume;
- nel traffico veicolare;
- nell'uso in contemporanea di cellulari, telefoni e apparecchiature rumorose.

I lavoratori nella scelta del posto di lavoro devono quindi privilegiare quelli meno rumorosi.

RISCHIO ELETTRICO

Durante l'esecuzione della prestazione lavorativa in Lavoro Agile i lavoratori devono porre in essere comportamenti adeguati a limitare il rischio elettrico. Di seguito sono elencate alcune misure che occorre adottare per ridurre il rischio elettrico:

- prese, interruttori ed apparecchiature elettriche devono essere mantenuti integri e ben fissati alle pareti;
- le apparecchiature devono essere utilizzate in conformità con le istruzioni d'uso fornite dal costruttore nel Manuale d'Uso e Manutenzione che ogni attrezzatura ha a disposizione;
- l'utilizzo di prese multiple con numerose spine collegate è da evitarsi o comunque è subordinato alla verifica che la potenza complessiva delle apparecchiature collegate sia compresa entro i limiti indicati sulle prese o sulle ciabatte stesse;
- deve essere evitato l'uso di prese o apparecchiature elettriche in situazioni in cui potrebbero trovarsi a contatto con acqua o altri liquidi conduttori;
- l'inserimento o il disinserimento delle prese elettriche devono avvenire ad apparecchiatura spenta e, in ogni caso, il disinserimento della presa non deve MAI avvenire tirando il cavo elettrico, ma impugnando correttamente la spina;
- verificare quali prese di corrente elettrica è possibile utilizzare per alimentare la propria attrezzatura informatica: non scollegare in autonomia apparecchiature presenti nel luogo presso cui si opera;
- nella scelta della presa elettrica da utilizzare verificare prima la compatibilità con la spina da collegare; nel caso queste non siano compatibili è necessario utilizzare gli appositi adattatori;
- è vietato l'utilizzo di prese multiple collegate in cascata.

POSTAZIONE DI LAVORO

Il lavoro al videoterminale può causare l'insorgenza di disturbi muscolo scheletrici e affaticamento visivo.
Per evitare l'insorgenza di queste problematiche gli elementi che possono incidere in maniera sostanziale sono i seguenti:

Il piano di lavoro

Come condizione generale, il piano di lavoro deve essere di ampiezza tale da poter disporre convenientemente tutti gli strumenti necessari all'attività, consentendo la necessaria libertà di movimento per utilizzarli agevolmente, e permettere l'appoggio delle mani e delle braccia (serve uno spazio di appoggio di circa 10-20 cm). Il lavoratore deve poter utilizzare i diversi dispositivi mantenendo sempre una posizione confortevole, senza dover estendere o ruotare in modo improprio il corpo. Al di sotto del piano deve esserci lo spazio per un comodo movimento delle gambe, per permettere di cambiare posizione durante l'attività (si consideri una profondità di almeno 70 cm, con uno spazio tra le cosce e la parte inferiore del piano). Il piano di lavoro deve essere inoltre stabile, in grado di sostenere tutto il materiale d'uso, ma anche sostenere senza cedere o ribaltarsi il peso di una persona che si appoggi su un bordo o su un angolo. Come ulteriore indicazione, il piano non deve avere spigoli vivi, ma arrotondati. Per quanto riguarda l'altezza, in condizioni ottimali dovrebbe essere regolabile a seconda delle esigenze del lavoratore ma in generale deve essere tale da permettere che il lavoratore mantenga la schiena
diritta e le braccia possano essere verticali, con gli avambracci paralleli al piano stesso, eventualmente appoggiati sul piano (anche grazie alla regolazione adeguata della seduta ed eventualmente l'uso di un poggiapiedi). La superficie deve essere opaca, per evitare possibili fastidiosi fenomeni di riflessione, e deve essere di un colore adeguato (possibilmente chiaro) che consenta un immediato riconoscimento di quanto presente sul piano stesso, in relazione all'attività che si deve svolgere.

Sedili di lavoro

Il sedile di lavoro è fondamentale perché la postura assunta durante il lavoro sia corretta, in modo da minimizzare i possibili danni dovuti al fatto di mantenere per lunghi periodi una posizione seduta; deve fornire un supporto stabile ma deve anche permettere i cambiamenti di posizione (non devono esserci posizioni obbligate), inoltre deve avere caratteristiche che ne rendano confortevole l'uso. Secondo le indicazioni del D.lgs. 81/08 il sedile deve essere di altezza regolabile, con gli spazi della seduta adattabile all'utilizzatore (quindi profondità della seduta e larghezza e altezza dei braccioli), avere un supporto lombare con altezza e inclinazione regolabili, avere superfici con bordi smussati, essere girevole per facilitare i cambi di posizione senza dover ruotare la colonna vertebrale, ed essere facile da spostare. Seduta e schienale devono essere in materiale traspirante, e tutto deve essere di facile pulizia. Altre indicazioni relative al sedile riguardano la resistenza allo scivolamento della seduta (non deve essere possibile scivolarne fuori involontariamente), la presenza di una base a 5 razze antiribaltamento e di rotelle per facilitare gli spostamenti (sia per entrare e uscire dalla postazione, sia per spostarsi ad esempio per prendere un oggetto). La sedia non deve potersi spostare accidentalmente, o quando non è occupata: le caratteristiche di attrito delle rotelle vanno valutate a seconda delle caratteristiche del pavimento. Per alcune condizioni di lavoro in cui si usa la posizione reclinata (ad esempio controllo di schermi posti più in alto della testa) lo schienale deve fornire un supporto sicuro anche per le scapole. I braccioli devono essere regolabili e, soprattutto, non devono essere un ostacolo alla vicinanza con il piano di lavoro (devono permettere che la sedia entri sotto il piano di lavoro).

CRITERI PER LA PREVENZIONE DI DISTURBI VISIVI

Secondo i dati epidemiologici, l'uso corretto di Videoterminali (VDT) non comporta di norma danni permanenti all'occhio umano.

Il disagio rilevato da alcuni lavoratori dopo un uso prolungato del computer è essenzialmente conseguente a un fenomeno di stanchezza che non ha ripercussioni sullo stato di salute dell'occhio. Tra i fattori ambientali che possono contribuire ad accrescere il disagio visivo di chi utilizza un VDT si segnalano:

- l'impostazione non adeguata del contrasto e della luminosità dello schermo;
- la presenza di un'illuminazione generale inappropriata e di un ambiente circostante che favorisce la presenza di riflessi, abbagliamenti e zone d'ombra.

Nella scelta del posto di lavoro i lavoratori privilegeranno i luoghi ben illuminati e nei quali l'illuminazione sia uniforme ovvero i luoghi privi di zone d'ombra oltre a porre in essere le seguenti misure di prevenzione di carattere ambientale e comportamentale:

- Il monitor deve essere posizionato in maniera da evitare abbagliamenti diretti o di riflesso con le fonti luminose;
- video e documenti devono essere posizionati a una distanza dagli occhi compresa tra 50 e 70 cm o diversa nel caso di soggetti che utilizzano lenti o occhiali;
- il monitor deve essere posizionato di fronte (lo spigolo superiore dello schermo deve essere un po' più in basso della linea orizzontale che passa per gli occhi dell'operatore) e a una distanza dagli occhi pari a circa 50 - 70 cm;
- il monitor deve essere liberamente e facilmente orientabile, inclinabile e regolabile in altezza (mediante apposito supporto nel caso si utilizzi un PC portatile);
- lo schermo deve essere mantenuto "a fuoco" e deve essere posizionato in maniera tale da trovarsi ad angolo retto rispetto alle fonti di luce naturali e artificiali in modo da evitare riflessi e abbagliamenti;
- il lavoratore deve preoccuparsi di distogliere periodicamente lo sguardo dal video e, durante le pause, deve privilegiare le attività meno impegnative sul piano visivo;
- tastiera, mouse e schermo devono essere regolarmente puliti e possibilmente separati dal corpo del VDT nel caso in cui si utilizzi un PC portatile.

CRITERI PER LA PREVENZIONE DI DISTURBI OSTEOMUSCOLARI

La maggior parte delle problematiche di salute causate dall'uso di VDT sono riconducibili alla postura assunta dal lavoratore durante il lavoro. Posizioni di lavoro inadeguate dovute sia ad un'errata disposizione degli arredi e del terminale che al mantenimento della stessa posizione per periodi prolungati, possono portare all'insorgere di disturbi a carico del collo, della schiena, delle spalle e delle braccia in chi utilizza i VDT. Anche in questo caso la prevenzione passa attraverso interventi di carattere ambientale e comportamentale. Il lavoratore deve assumere una postura corretta davanti al video mantenendo:

- i piedi ben poggiati al pavimento;
- le ginocchia piegate a formare un angolo di 90°;
- la schiena appoggiata allo schienale nel tratto lombare;
- la testa non costantemente inclinata;
- gli avambracci appoggiati al piano di lavoro e un angolo di 45° tra braccia e busto per evitare l'irrigidimento di polsi (che devono stare sempre diritti) e dita;
- posizioni fisse per tempi non eccessivamente prolungati (può essere sufficiente al riguardo allungare semplicemente le gambe ogni tanto, alzarsi ecc.).

SPAZI DI LAVORO E VIE DI FUGA

Nella scelta dello spazio di lavoro è necessario prestare attenzione a:

- corretto posizionamento dei cavi di alimentazione del computer, in modo tale da evitare il pericolo di inciampo e quindi di eventuali cadute;
- avere spazi sufficienti per alzarsi e spostarsi senza rischiare di urtare contro mobili e spigoli;
- evitare di posizionarsi nello spazio di apertura di porte e armadi;
- verificare di avere a disposizione vie di fuga agevoli e prive di ostacoli;
- evitare luoghi di lavoro troppo caldi o troppo freddi o comunque con condizioni microclimatiche inadeguate;
- evitare luoghi di lavoro con superfici illuminanti (serramenti esterni) prive di schermatura;
- evitare luoghi di lavoro con illuminazione naturale/artificiale insufficiente.

GESTIONE DELL'EMERGENZA

Il lavoratore deve evitare di scegliere di prestare l'attività lavorativa in luoghi isolati e remoti e dovrà avere sempre a disposizione un mezzo per la chiamata dei soccorsi. Nel caso in cui l'attività venga prestata in locali pubblici e/o privati nei quali è presente un piano di emergenza, occorre individuare le vie e le uscite di emergenza e la relativa segnaletica, cercare di capire le modalità di attivazione dell'allarme evacuazione e seguire le indicazioni degli Addetti all'Emergenza del posto in cui ci si trovi.

AMBIENTI DI LAVORO ESTERNI

Il lavoratore che svolge attività di Lavoro Agile si espone a rischi per la propria salute e sicurezza laddove il luogo prescelto per l'esecuzione della prestazione comporti:

- esposizione diretta alle radiazioni solari;
- esposizione prolungata a condizioni meteoclimatiche sfavorevoli (caldo o freddo intensi, elevata umidità);
- svolgimento dell'attività in luoghi isolati o in cui sia difficoltoso richiedere e ricevere soccorso;
- svolgimento dell'attività in luoghi con presenza di animali o che non siano adeguatamente manutenuti con riferimento alla vegetazione, al degrado ambientale, alla presenza di rifiuti, etc.;
- svolgimento di attività in aree con presenza di sostanze pericolose, combustibili o infiammabili e sorgenti di ignizione;
- svolgimento di attività in aree con transito di mezzi;
- svolgimento di attività con rischio di aggressione;
- svolgimento di attività in aree in cui non ci sia la possibilità di approvvigionarsi di acqua potabile.

Il lavoratore deve impegnarsi a evitare luoghi di lavoro all'esterno che lo espongano ai rischi sopra menzionati, organizzando la propria posizione secondo le indicazioni fornite ai punti precedenti.

SEGNALAZIONE INFORTUNI

Nel caso in cui il/la lavoratore/trice agile sia oggetto d'infortunio deve fornire dettagliata e tempestiva informazione sull'evento, secondo le modalità definite per tutto il personale .

Allegato A2

POLICY PER LA SICUREZZA INFORMATICA E PER L'UTILIZZO DEGLI STRUMENTI INFORMATIVI E TELEMATICI

REGIONE MARCHE

POLICY PER LA SICUREZZA INFORMATICA

E PER L'UTILIZZO DEGLI STRUMENTI INFORMATIVI E TELEMATICI

DOCUMENTO FINALIZZATO ALLA CONFORMITÀ ALLO STANDARD UNI CEI ISO/IEC 27001:2013

REV.	DATA	DESCRIZIONE	APPROV.
1.0	08.01.2021	Prima emissione	

NOTE REVISIONE / EDIZIONE / APPLICAZIONE

SOMMARIO

1 Disposizioni generali

1.1 Definizioni

Termini	Definizione
AdS	Amministratore di Sistema
Backup	Salvataggio periodico e programmato dei dati
Collaboratori	I dipendenti della Regione Marche, senza distinzione di ruolo, inquadramento, contratto, modalità di assunzione e/o livello e qualifica professionale, i collaboratori esterni quale che sia il rapporto contrattuale instaurato con l'amministrazione regionale (contratti di collaborazione coordinata e continuativa, stage, tirocini, incarichi libero-professionali, consulenza, stage ecc,), i dipendenti e collaboratori dei fornitori di beni e servizi all'amministrazione regionale
Disaster recovery	Ripristino del sistema e dei dati a seguito di un evento distruttivo
Freeware	Software distribuito gratuitamente e senza bisogno di licenza d'uso, per lopiù reperibile attraverso Internet.
Guest book	Libro degli ospiti inteso in informatica come un sito dove poter lasciare ipropri dati per esprimere un giudizio o commento
Host	Singola istanza di servizi (applicazioni) che sono erogate dagli apparati di elaborazione cioè le macchine server fisiche
IAM	Identity Access Management – sistema di gestione e controllo dell'identitàdegli accessi alla rete informativa
ICT	Information & Communication Technology – Tecnologie Informatiche e di Comunicazione
LOG	Registrazione in un elenco delle attività di un computer o di un suo utente
Nick name	Nominativo (o soprannome) utilizzato tipicamente per la registrazioneutente su servizi on-line
SCCM	Sistema di gestione che consente di gestire un numero elevato di computerin esecuzione su vari sistemi operativi
Shareware	Software che può essere provato gratuitamente, pur rimanendo vincolatoal diritto d'autore
Sistema informativo interno	si intende sia la rete interna, sia ogni strumento informatico ad esso collegato (pc, tablet, telefoni…)
VPN	Sistema di collegamento alla rete aziendale (Virtual Private Network)dall'esterno della stessa

1.2 Riferimenti

- PSG – Politica per la Sicurezza delle Informazioni
- PO01 – Processo di Gestione degli Accessi "Identity and Access Management"

1.3 Finalità

La presente policy è finalizzata:

- illustrare e disciplinare le modalità di utilizzo del sistema informativo interno della ***Regione Marche***;
- regolamentare le modalità di fruizione dei servizi che, tramite i sistemi ICT, è possibile ricevereo offrire all'interno e all'esterno dell'organizzazione;
- descrivere la gestione dei dati personali;
- identificare e garantire i diritti dell'interessato in ottemperanza alla legislazione sulla privacy;
- stabilire regole generali sui concetti di sicurezza informatica ed informativa;
- dichiarare lo stato di possesso e proprietà dei dati in gestione al termine della collaborazione professionale.

Il presente documento stabilisce, altresì, le regole interne in relazione alla protezione dei dati personalie delle informazioni in generale, agli obblighi di riservatezza, e quindi alle regole di gestione delle attività quotidiane afferenti a quanto sopra indicato.

1.4 Ambito di applicazione

La presente policy si applica a tutti i Collaboratori, salvo quanto espressamente specificato nel presente documento e con riferimento all'intero novero di strumenti, servizi e apparati informatici e di gestione/trattamento di dati ed informazioni, anche se non ancora diffusi sul mercato, che rientrano o rientreranno nella definizione di "Rete Informatica" e/o "Risorse ICT" o che potranno comportare rischie problemi per la sicurezza o protezione dei dati ed informazioni.

1.4.1 Rete ICT Interna

La rete ICT (*Information & Communication Technology*) interna è rappresentata dagli strumenti, apparecchiature, software o quant'altro sia utilizzabile per "comunicare" e per gestire "informazioni".

Tutte le considerazioni e regole relative alla rete ICT interna sono applicabili anche alla rete WIFI interna.

1.4.2 Strumenti ICT

Gli strumenti ICT sono messi a disposizione dei dipendenti esclusivamente per lo svolgimento dell'attività aziendale demandata loro.

Il controllo sui suddetti strumenti, alle condizioni di legge e con le modalità previste nel presente attoè necessario ai fini dell'assicurazione da un lato dell'efficienza dell'azione amministrativa, dall'altro della sicurezza della trasmissione e della conservazione dei dati che l'amministrazione gestisce e infine della sicurezza del lavoro stessa.

2 Linee guida e misure tecniche ed organizzative

2.1 Figure e ruoli all'interno della OrganizzazioneRegionale

Sono individuate le seguenti figure interne all'organizzazione regionale alle quali sono affidati compitie funzioni in materia di sicurezza informatica,

- Responsabile della sicurezza Informatica
- ISMS Manager
- Responsabili di funzione e/o posizione organizzativa
- Responsabile ICT
- Referenti informatici di Struttura
- Dirigenti – Delegati al Trattamento dei dati personali
- Amministratori di sistema (AdS)
- Responsabile della protezione dei dati

Inoltre vengono individuati i seguenti soggetti esterni con compiti incidenti sulla sicurezza informaticae protezione dei dati :

- Responsabile esterno del trattamento
- Contitolari
- Titolari del trattamento (che nominano l'organizzazione Responsabile del trattamento)

Le funzioni e compiti assegnati a ciascuna figura sono disciplinate oltreché dal presente atto, dagli ulteriori atti e provvedimenti amministrativi in materia già adottati dall'Amministrazione Regionale, anche relativamente all'adeguamento alla normativa sulla protezione dei dati personali (Reg.Ue 679/2016)

2.2 Sistema dei controlli

2.2.1 Gradualità

Qualora, nonostante le misure tecniche e organizzative preventivamente adottate dall'Amministrazione regionale, si verifichino o possano verificarsi eventi dannosi o situazioni di pericolo per la sicurezza e riservatezza dei dati e delle informazioni, la stessa effettuerà con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

a) analisi aggregata del traffico di rete riferito all'intera Rete Informatica o a sue aree (reparto, servizio, ecc.), rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni) dei dati memorizzati sui server a livello di intera struttura lavorativa (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini,software non autorizzato) dei dati memorizzati su client e relativa pertinenza con l'attività lavorativa;
b) emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti interni, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori

afferenti al settore in cui è stata rilevata l'anomalia;

c) in caso di successivo permanere di una situazione non conforme e in caso di abusi singoli e reiterati, si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro. Sarà possibile procedere con un'analisi puntuale ed una eventuale eliminazione del materialenon conforme anche sulle singole postazioni di lavoro e sugli strumenti informatici in dotazione al singolo lavoratore o collaboratore, alle condizioni sotto indicate. In caso di accertati abusi si procederà anche alla segnalazione all'Ufficio Provvedimenti Disciplinari.

2.2.2 Controlli sui dispositivi in dotazione ai Collaboratori

L'Amministrazione Regionale può procedere a controlli sull'attività dei Collaboratori, nei limiti consentiti dalle norme legali e contrattuali e nel rispetto dei diritti dei lavoratori, per le seguenti finalità:

- verifica dell'integrità della propria Rete Informatica
- verifica dell'ottemperanza di disposizioni di legge e contrattuali
- verifica del rispetto delle disposizioni relative alla sicurezza informatica ed alla protezione dei dati personali e di quanto previsto dal presente documento

I controlli vengono effettuati attraverso personale della struttura competente in materia ICT previamente individuato e autorizzato, accedendo a dati e a informazioni contenute nei dispositivi informatici / tecnologici in dotazione ai Collaboratori stessi (PC, Notebook, tablet, smartphone,Blackberry, badge elettronici,…).

Le operazioni sui dispositivi informatici e tecnologici in dotazione devono essere effettuate in modo anonimo. L'individuazione nominativa del Collaboratore è ammessa solo se strettamente necessaria per le finalità indicate nel presente documento.

Qualsiasi intervento effettuato sui dispositivi in dotazione, dovrà essere documentato e verbalizzato nelle forme più idonee, indicando le motivazioni dell'accesso e le informazioni, dati e documentazioneeventualmente estratti, e mettendo tale documentazione a disposizione del Collaboratore interessato.

Per tutti i fini connessi al rapporto di lavoro, inclusa la facoltà di emettere provvedimenti disciplinari, èammesso il controllo e la verifica da parte dell'Amministrazione Regionale sugli strumenti informatici in dotazione ai dipendenti dell'Amministrazione regionale, senza necessità di previo accordo sindacale,a condizione che esso non si traduca in un controllo a distanza dell'attività e che sia data al lavoratoreadeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispettodi quanto disposto dal regolamento UE 679/2016 e dal decreto legislativo 30 giugno 2003, n. 196.

2.2.3 Controlli per finalità tecniche e/o amministrative

Fermo quanto sopra, l'accesso da parte dell'Amministrazione Regionale ai dati e informazioni trattati dai Collaboratori attraverso la Rete Informatica può avvenire, al di fuori di ogni finalità di controllo preventivo e sistematico dell'attività lavorativa e nel rispetto della normativa a tutela della protezione dei dati personali, anche per:

a) motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione diprogrammi, manutenzione hardware, etc.);
b) controllo o programmazione dei costi;
c) comprovate esigenze manageriali o lavorative (ad es. accesso al computer del Collaboratore

per reperire file necessari all'attività lavorativa che siano conservati esclusivamente "in locale"su detto dispositivo, nel caso di assenza non programmata del Collaboratore);

d) permettere il libero accesso alle informazioni tanto della rete internet che della postaelettronica anche all'Autorità Giudiziaria richiedente.

2.2.4 Accesso da remoto

Per motivi di assistenza, manutenzione, ricerca virus, attività di indagine sui malfunzionamenti, ricercadi anomalie o altre esigenze dell'organizzazione, la struttura competente in materia ICT può accedereda remoto sui dispositivi collegati alla rete interna o dall'esterno mediante connessione VPN o con SCCM.

L'accesso sul dispositivo da parte della struttura competente normalmente viene concordato con il collaboratore che ne richiede la teleassistenza. Tuttavia, in talune circostanze dettate da comprovata urgenza, la struttura competente in materia ICT potrà collegarsi sui sistemi senza nessuna specifica autorizzazione preventiva o comunicazione in tal senso.

2.2.5 Log degli accessi

Tutti i sistemi informatici interni sono configurati per effettuare dei LOG sulle attività e sulla connettivitàal fine primario di tutelare la sicurezza informatica dell'ente regionale. Tali sistemi di registrazione includono gli accessi ai sistemi, alla posta elettronica, alle connessioni di rete verso sistemi interni, alleconnessioni di rete verso host esterni, all'utilizzo di file all'interno delle cartelle condivise, ecc.

I LOG potranno essere sottoposti ad analisi, monitoraggio e verifica dal personale della struttura competente in materia ICT, amministratore di sistema o qualsiasi altra persona fisica e giuridica, sololaddove sia assolutamente necessario e/o specificatamente e motivatamente richiesto.

I dati contenuti nel LOG sono assolutamente anonimi, ma consentono di identificare il PC e/o utente in locale ad una connessione a servizi interna o esterna. E' pertanto assicurata la separazione tra i sistemi di effettuazione dei LOG e quelli contenenti gli indirizzi IP dei dispostivi in dotazione dei Collaboratori, in modo da evitare qualsiasi possibilità di identificazione nominativa in automatico in occasione di operazioni di monitoraggio e verifica dei log.

2.3 Proprietà degli strumenti / risorse informative

Le risorse informative interne (fisiche, logiche o virtuali – asset, dato o informazioni) sono e rimarrannodi proprietà dell'Amministrazione Regionale e l'assegnazione e disponibilità delle stesse sono "temporanee", nonché limitate all'esclusivo uso professionale. L'assegnazione delle risorse non implicaun trasferimento del diritto di proprietà, di usufrutto, di comodato d'uso delle stesse, non provoca la nascita di un diritto di esclusiva sull'utilizzo, né tantomeno deve essere considerata come benefit sulla retribuzione o come l'autorizzazione all'utilizzo promiscuo.

In caso di comprovata necessità, ad esempio in caso di assenza prolungata imprevista o di necessitàal fine della continuità operativa, l'Amministrazione regionale può:

- revocarne l'utilizzo;
- cancellarne i dati;

- assegnarli ad altro personale;
- modificarne gli accessi;
- modificarne le condivisioni;
- svolgere attività di controllo, amministrazione, backup.

La consegna di una risorsa viene formalizzata e verbalizzata con la redazione di un apposito modulo in cui viene identificata la risorsa consegnata.

2.4 Regole generali in materia di domicilio informatico-digitale, identità digitale e posta elettronica

L'Amministrazione Regionale mette a disposizione dei Collaboratori sia caselle di posta di tipo condiviso, quali amministrazione@organizzazione.it, oppure xxx.regione@organizzazione.com, ma anche alle caselle di posta nominali quali nome.cognome@organizzazione.it.

L'indirizzo nome.cognome@organizzazione.it non appartiene a colui identificato con "nome.cognome",bensì alla proprietaria del dominio, ovvero la "organizzazione.it".

Fermo restando che la riservatezza di una casella di posta elettronica "personale privata" è tutelata a livello costituzionale, in ambito civile e penale e dalla normativa in materia di protezione dei dati, quando la casella di posta è messa a disposizione da parte dell'Amministrazione regionale, quest'ultima può accedere alle informazioni ivi contenute per le finalità indicate al punto 2 del presenteatto, nonché per comprovate esigenze lavorative e d'ufficio, alle seguenti condizioni:

1) il Collaboratore deve essere preventivamente avvisato, con modalità idonea a garantirne l'effettiva informazione, della facoltà dell'Amministrazione regionale di accedere alla sua casella e-mail e alla relativa corrispondenza;
2) il controllo delle e-mail non può superare i limiti imposti dalla finalità del trattamento, ragione per cui il controllo deve essere limitato alla corrispondenza attinenti alle questioni che coinvolgono l'amministrazione e che hanno reso necessario l'intervento;
3) l'Amministrazione deve consentire la "tracciabilità dei controlli", in modo da rendere chiaro quanti e quali messaggi sono stati monitorati, per quanto tempo e quante persone hanno avuto accesso ai risultati della sorveglianza;
4) deve essere rispettato il principio di proporzionalità tra finalità perseguita e tutela della riservatezza, per cui non sono consentiti controlli massivi, attivati in assenza di un motivo specifico o di un pericolo attuale.
5) nel caso di fondato sospetto di infedeltà del Collaboratore, al fine della ricerca di elementi oggettivi comprovanti la stessa.

Nel caso in cui il collaboratore, per cessazione del rapporto di lavoro o di collaborazione o per qualsiasialtro motivo, non svolga più attività all'interno dell'Amministrazione Regionale, quest'ultima manterrà la casella di posta del collaboratore attiva per due mesi, previa modifica della password di accesso. Intali casi verrà impostato un messaggio automatico in cui siano fornite tutte le indicazioni utili e, in particolare, il recapito mail del collaboratore di riferimento in sostituzione.

Decorsi due mesi, l'account verrà disabilitato, disattivando anche il messaggio di risposta automatica.

L'Amministrazione Regionale potrà accedere ai contenuti della casella di posta disattivata per un periodo massimo di 3 mesi.

Nessuna comunicazione sarà garantita al collaboratore la cui casella di posta sia stata revocata e/o reindirizzata verso un altro destinatario.

Tutte le disposizioni relative alle caselle di posta elettronica interna assegnata al Collaboratore devonoritenersi valide, per quanto compatibili, anche per qualsiasi altro strumento di messaggistica/corrispondenza elettronica messo a disposizione dalla Amministrazione ai Collaboratori.

2.5 Cessazione dei servizi

Ai sensi del presente regolamento, le credenziali di accesso alla rete informatica interna, a specifici software, così come l'utilizzo del servizio di accesso ad internet e di utilizzo della posta elettronica, potranno essere cessati o limitati anche temporaneamente, fermo restando gli eventuali provvedimentidisciplinari da adottarsi, nei seguenti casi:

a) se non sussiste più la condizione di Collaboratore autorizzato o non è confermata l'autorizzazione all'uso;
b) se è accertato un uso non corretto delle risorse informatiche da parte del Collaboratore o comunque un uso estraneo ai suoi compiti professionali;
c) se vengono sospettate manomissioni e/o interventi sull'hardware e/o sul software da parte del Collaboratore, anche per il tramite di personale non autorizzato;
d) in caso di diffusione o comunicazione, imputabili direttamente o indirettamente al Collaboratore, di password e/o altre informazioni tecniche riservate;
e) in caso di accesso intenzionale dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli autorizzati e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale, all'Amministrazione Regionale;
f) in ogni altro caso in cui sussistono ragionevoli evidenze di una grave violazione dei propri obblighi da parte del Collaboratore.

2.6 Installazione ed utilizzo dei SoftWare

All'interno dell'organizzazione, in merito all'installazione/utilizzo dei software, la struttura competentein materia ICT ha la responsabilità di:

- valutare le necessità in ambito ICT;
- scegliere la soluzione più idonea;
- valutare l'impatto sulla sicurezza;
- acquistare il software necessario;
- gestire le licenze;
- provvedere all'installazione sui PC dei collaboratori;
- gestire gli aggiornamenti;
- valutare l'acquisto di nuove versioni per adeguamento a criteri di sicurezza o funzionalità.

Alla luce della predetta responsabilità esclusiva della struttura ICT, è vietato l'utilizzo/installazione di qualsiasi software/applicazione non precedentemente autorizzato dalla struttura stessa.

Con un apposito modulo che sarà disponibile online il dirigente dovrà richiedere l'autorizzazione di

installazione per software necessari ai fini lavorativi.

In caso di installazione di software pericolosi o con licenza non regolare, rilevati all'interno delle macchine di proprietà dell'organizzazione, sarà effettuata una immediata rimozione degli stessi, valutando sia eventuali sanzioni disciplinari, sia segnalazioni alle autorità nei casi più gravi.

2.7 Protezione della rete telematica Regionale, della serverfarm e delle postazioni

2.7.1 Tutela riservatezza, integrità, disponibilità e resilienza dellarete telematica – Backup

Al fine di garantire riservatezza, integrità, disponibilità e resilienza della rete telematica regionale, delle singole postazioni dell'ente e della server farm sono stati installati ed attivati strumenti generali didifesa informatica per:

- adottare un controllo degli accessi logici (in ingresso ed in uscita);
- garantire solo l'accesso autorizzato alle risorse informatiche;
- utilizzare sistemi ridondanti a diversi livelli per garantire continuità nell'erogazione dei servizi;
- integrare politiche di backup e verifica del disaster recovery periodiche;
- adottare misure tecniche ed organizzative per minimizzare le interruzioni di servizio.
- Implementare una topologia di rete che effettua delle partizioni logiche dei diversi ambienti;
- controllare nominalmente i criteri di accesso alla struttura di rete tramite VPN.

I pc collegati alla rete regionale sono adeguati automaticamente agli ultimi aggiornamenti critici e di sicurezza, sia per il sistema operativo che pe le applicazioni di office.

L'utente che si collega alla sua postazione di lavoro non può avere i diritti di amministratore locale. Attraverso l'utilizzazione di appositi software centralizzati, sono individuate, da remoto, eventuali anomalie ed irregolarità, autorizzando i soggetti competenti (amministratori di sistema, tecnici autorizzati e referenti informatici):

- a disinstallare i software non autorizzati o privi di regolare licenza;
- eliminare eventuali amministratori locali e a togliere i diritti di amministratore locale se presenti;
- in caso estremo, isolare postazioni che dovessero risultare anomale o non regolari.

2.7.2 Amministratori di Sistema

Sono individuati e rivisti periodicamente gli elenchi degli amministratori di sistema, le competenze e la validità dei requisiti di accesso relativamente alle singole postazioni dell'ente ed alla server farm, ad eccezione dei trattamenti affidati a responsabili esterni che provvedono direttamente per competenza.

Ciascun dirigente di servizio o P.F. dovrà provvedere alla nomina, ad AdS dei propri dipendenti che svolgano tali funzioni e agli ulteriori incombenti previsti dal provvedimento Garante Privacy 27/11/2008,valutando, con il supporto della P.F. Informatica, i requisiti di esperienza, capacità e affidabilità del soggetto designato.

2.7.3 Separazione dati anagrafici e particolari - pseudonimizzazione, cifratura, minimizzazione

Nel rispetto della disciplina in materia di tutela dei dati personali a fronte di richieste specifiche da partedei dirigenti delegati, viene dato supporto per verificare e segnalare che i fornitori assicurino la separazione tra dati anagrafici e dati appartenenti a categorie particolari dei software operativi e dei programmi applicativi, ovvero la cifratura dei dati idonei a rivelare lo stato di salute e la tracciabilità dell'attività degli utenti.

La P.F. Informatica supporta ciascun dirigente delegato al trattamento nell'adozione, se necessario, dimisure di pseudonimizzazione, cifratura, minimizzazione ed in ogni altra tecnica di anonimizzazionedei dati trattati, con riferimento anche al parere 10/04/2014 del gruppo ex art.29 della direttiva 95/46.

2.7.4 Verifica adeguatezza al principio della "Privacy by design"

Nel rispetto della disciplina in materia di tutela dei dati personali potranno essere valutate a campioneo a fronte di richieste specifiche da parte dei dirigenti delegati, l'adeguatezza dei progetti rispetto ai principi dell'art.25 del RGDP ("Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita") nonché alla conformità agli obiettivi indicati nel Piano triennale per l'informatica nella pubblica amministrazione.

2.8 Disciplina dell'accesso alla rete telematica interna

2.8.1 Regole specifiche

Oltre alle disposizioni qui presenti, si rinvia per un ulteriore approfondimento al processo di gestione degli accessi realizzata al fine del Sistema di Gestione della Sicurezza delle Informazioni (processo PO01 – Processo di Gestione degli Accessi "Identity and Access Management")

2.8.2 Regole di accesso alla rete informatica

L'accesso alla rete informatica Interna, che è e deve essere sempre protetto da password, è limitato ai collaboratori e agli altri soggetti espressamente autorizzati dall'Amministrazione regionale con il supporto della struttura interna competente in materia ICT interna.

L'autorizzazione all'accesso al sistema informativo è data dalla struttura ICT interna. Nessuno al di fuori della stessa è autorizzato a rilasciare accessi o password atti ad accedere a qualunque sistema,compreso il Wi-Fi per gli ospiti.

Username e password per accedere alla rete ICT interna o a risorse digitali in qualsiasi forma, sono strettamente personali e il collaboratore è tenuto a tutelare e a mantenere la segretezza delle proprie credenziali di accesso.

La prima password di accesso viene fornita all'utente direttamente dal sistema ICT. Tale password dovrà essere cambiata al primo accesso da parte dell'utente stesso, secondo le regole di cui ai successivi punti, e viene custodita secondo le modalità più opportune definite dallo staff ICT.

2.8.3 Regole di accesso alla rete fisica

Tutte le postazioni di lavoro collegate alla rete fisica della Regione Marche devono utilizzare un insiemedi servizi di rete (Microsoft Active Directory su dominio "regionemarche.intra") per garantire il rispetto di criteri di gruppo, una gestione delle autenticazione alla rete aziendale centralizzata e la distribuzione automatica degli aggiornamenti, delle politiche di sicurezza e dei software antivirus ed antimalware.

La policy di accesso al dominio prevede l'attivazione automatica della complessità della password e della scadenza forzata ogni 85 giorni.

Per evitare attacchi "brute force" è stato introdotto il "lockout" dell'utente dopo 25 tentativi di inserimentodella password.

Se il Dirigente di struttura autorizza un collaboratore all'accesso alle risorse di dominio regionale (caselle di posta, cartelle condivise di rete, accesso a banche dati o applicativi ecc.) lo fa sotto la propria responsabilità vigilando costantemente l'operato dell'utente, impartendo apposite istruzioni e vincoli contrattuali che garantiscano l'applicazione delle misure di sicurezza tecniche e organizzative, la riservatezza delle informazioni e dei dati che tratteranno e la divulgazione non autorizzata.

Sono adottati meccanismi di controllo automatico dell'accesso alla rete di postazioni "fuori dominio" (eventualmente isolandole) e possono essere utilizzati solo indirizzi di rete preventivamente comunicatidalla struttura competente in materia ICT.

2.8.4 Autenticazione tramite Cohesion

È resa disponibile una piattaforma di autenticazione, attualmente denominata Cohesion, per assicurare ai sistemi informativi di settore la possibilità di integrarsi con un unico sistema standard tecnico ed organizzativo comune. I profili autorizzativi sono gestiti informaticamente in base alla profilazione degli utenti secondo la modulistica disponibile nella intranet regionale.

2.8.5 Regole di "Password Change"

Il Collaboratore è tenuto a sostituire la propria password ogni volta che sospetta che la stessa non siapiù segreta. La password deve essere cambiata almeno una volta ogni 85 giorni.

Nel caso in cui, per motivi tecnici od organizzativi, non sia possibile cambiare in autonomia la passwordai sistemi, è responsabilità di ogni collaboratore richiedere l'intervento della struttura competente in materia ICT.

Le password devono essere formate da lettere (maiuscole o minuscole, con rilevanza ai fini del sistema), numeri e caratteri speciali; devono essere composte da almeno otto caratteri alfanumerici di cui almeno un numero, una lettera maiuscola e una lettera minuscola e non devono contenere riferimenti agevolmente riconducibili al soggetto interessato.

Le password non devono contenere nomi o parti di nomi comuni (es. PIPPO, GIOVA, MARIA ecc.), sequenza di caratteri troppo semplici (es ABCD, QWERTY, 12345 ecc.) o riferimenti alla propria sfera personale (es. data di nascita, parti del codice fiscale, nomi dei figli ecc.).

Per una maggiore flessibilità nelle attività operative e nella gestione del sistema ICT, è data facoltà al personale di modificare secondo schemi e regole prestabilite la password di accesso ai sistemi

informativi.

Qualora il Collaboratore venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Dirigente di riferimento (o persona da questa incaricata) o alla struttura competente in materia ICT, oppure al custode delle password, ove previsto.

2.8.6 Regole di disattivazione

Le credenziali di autenticazione non utilizzate da almeno tre mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica, organizzativa o di servizio; anche in questo caso la struttura competente in materia ICT si fa garante della gestione degli account tecnici utilizzati.

Le credenziali sono disattivate anche in caso di "perdita della qualità" che consente al collaboratore incaricato l'accesso alle informazioni (per "perdita della qualità" si intende il deterioramento o perdita di caratteristiche essenziali della accoppiata "***login + password***" quali, ad esempio, segretezza, univocità, robustezza password, ecc. ecc.)

La cessazione degli utenti di dominio dovrà avvenire in maniera puntuale. Per gli Utenti di tipo "dipendente" (in possesso di matricola dipendente fornita dal Servizio Risorse Umane), la cessazioneavviene in automatico grazie alla sincronizzazione del database delle Risorse Umane con il servizio diautenticazione di dominio.

Per gli Utenti di tipo "collaboratore/consulente" (senza matricola dipendente), a cui sono state fornite le credenziali di dominio per l'accesso alle risorse di dominio (cartelle condivise su Ormadfs, caselle diposta generiche, accesso a database e ad applicativi quali Paleo, Openact ecc.), in caso di cessazionedel rapporto di collaborazione/consulenza, il Dirigente è obbligato ad avvisare immediatamente la struttura competente in materia ICT per l'immediata disattivazione dell'utente.

Il Dirigente deve porre la massima attenzione nel momento in cui: o per effetto di una riorganizzazioneo per lo spostamento di dipendenti da una struttura a un'altra, le autorizzazioni precedentemente assegnate all'utente alle risorse di dominio quali caselle di posta generiche/ufficiali, cartelle condivise(OrmaDfs), accesso a banche dati o applicativi quali Paleo, OpenAct ecc. vengano modificate opportunamente tramite l'apposita modulistica messa a disposizione dalla struttura competente in materia ICT

3 Modalità di utilizzo dei sistemi e mezzi telematici daparte di dipendenti e collaboratori

3.1 Custodia delle risorse

Le Risorse ICT interne (PC, portatili, smartphone, ecc), affidate ai collaboratori devono essere custodite con cura ed in modo appropriato, evitando ogni possibile forma di danneggiamento, manomissione o utilizzo da parte di soggetti terzi non autorizzati. Il furto, il danneggiamento o lo smarrimento delle Risorse ICT interne devono essere prontamente segnalati all'Amministrazione regionale.

Le Risorse ICT interne non devono essere lasciate incustodite durante una sessione di trattamento deidati. L'accesso alla postazione di lavoro deve essere bloccato ogni qual volta ci si allontani da essa (digitando sulla tastiera "CTRL+ALT+CANC"). La protezione del sistema interviene comunque in automatico dopo il periodo di inattività stabilito dalle policy. Il sistema deve essere sempre sotto controllo.

Al termine della giornata lavorativa, in caso di assenze prolungate o in caso di suo inutilizzo, il PC e lerelative periferiche (monitor, stampanti ecc.) devono essere spenti.

Oltre alle prescrizioni di cui al presente atto, tutti i Collaboratori sono tenuti anche all'osservanza delleregole di media diligenza, prudenza e perizia, propri del "buon padre di famiglia", in relazione a beni che non sono di proprietà individuale e che sono forniti in dotazione al Collaboratore unicamente per lo svolgimento delle proprie funzioni e dei propri compiti ed in costanza degli stessi

Qualunque violazione delle regole e disposizioni del presente atto saranno valutati, ed eventualmente sanzionati con provvedimenti disciplinari e risarcitori nel caso di personale dipendente, nonché attraverso gli appositi rimedi contrattuali nel caso di collaboratori esterni e/o fornitori.

3.2 Abuso e alterazione delle risorse ICT

Non è consentito utilizzare strumenti software e/o hardware, facenti parte delle Risorse ICT, al fine di intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti in qualsiasiforma e memorizzati in qualsiasi modalità, all'interno o all'esterno della rete dell'Amministrazione regionale

Non è consentita alcuna modificazione o alterazione dei sistemi operativi e delle configurazioni delle Risorse ICT. In particolare, ai Collaboratori non è consentito disinstallare, modificare, reinstallare, alterare o cedere/distribuire a terzi il sistema operativo ovvero qualsiasi altro software fornito in dotazione dall'Amministrazione Regionale, specialmente quando tali modifiche possanocompromettere la sicurezza della Rete ICT (ad es. disattivazione dell'anti-virus installato sul dispositivo) o violare la disciplina in tema di copyright.

3.3 Utilizzo condiviso delle risorse ICT

Qualora una Risorsa Infrastrutturale sia utilizzata da più autorizzati, ogni volta che è terminato l'utilizzodella stessa, ciascuno di essi dovrà disconnettersi dal sistema effettuando il *logout* del proprio profilo personale previa chiusura dei programmi rimasti eventualmente aperti in modo da dover ri-effettuare la procedura di autenticazione ad ogni nuovo accesso.

3.4 Cessazione del rapporto di lavoro

Al momento della cessazione del rapporto lavorativo il dipendente ha l'obbligo di riconsegnare immediatamente tutti gli strumenti e risorse ICT nello stato in cui gli sono stati consegnati, fatto salvo il normale deterioramento dovuto all'uso.

3.5 Obbligo alla riservatezza e al segreto professionale

Nella gestione ordinaria e straordinaria delle attività, tutti i collaboratori sono tenuti a garantire la massima riservatezza in relazione alle informazioni, dati usati o trattati per la loro attività o di cui vengano a conoscenza, direttamente o indirettamente.

Tutte le informazioni spedite e ricevute da ogni singolo collaboratore sono protette dal segreto d'ufficioo professionale. È pertanto tassativamente proibita la comunicazione o diffusione a persone o entità estranee all'Amministrazione regionale, se tale attività non sia stata esplicitamente prevista e autorizzata.

Nel caso in cui, per disposizioni di legge o di regolamento o per ordine di Autorità competenti, sia necessario inviare delle informazioni a soggetti terzi, dovrà essere preventivamente informata l'Amministrazione regionale ed anticipatamente concordati tempi e modalità di comunicazione.

La stampa dei messaggi o informazioni deve essere contenuta a quanto strettamente necessario per una corretta consultazione. Di norma, il documento cartaceo deve essere distrutto dopo la consultazione, salvo che esso sia utile per usi tecnici o di documentazione all'interno di specifici dossier. In caso di necessità di stampa, questa deve avvenire preferibilmente tramite il sistema di stampa riservata.

3.6 Informazioni Riservate e Accordi di Riservatezza

Per informazioni riservate si intendono tutte le informazioni riferite all'Amministrazione regionale, ai soggetti esterni e a qualsiasi collaboratore coinvolto anche indirettamente, identificate come tali dall'Amministrazione regionale stessa. A titolo esemplificativo e non esaustivo, esse sono: le informazioni scientifiche e/o tecniche riguardanti procedure, processi e know-how, prototipi realizzati, specifiche e dati, domande di brevetto depositate e ancora segrete, disegni, design e formule, informazioni, notizie, valutazioni, proposte, offerte, progetti, software e sistemi informatici, istanze, domande, osservazioni e quant'altro .

L'informazione può essere di qualsiasi forma, ossia verbale, scritta, informatica, digitale, immagini, suoni, ecc.

L'informazione è sempre classificata come "USO INTERNO" salvo diversa espressa indicazione.

La riservatezza si estende anche a informazioni riguardanti personale, collaboratori, clienti/utenti e fornitori dell'Amministrazione regionale

Ogni dipendente, collaboratore, fornitore esterno si impegna irrevocabilmente a non divulgare le informazioni riservate riferite all' Amministrazione regionale. Il soggetto esterno si impegna inoltre affinché anche i suoi dipendenti e consulenti esterni garantiscano la predetta riservatezza delle informazioni.

Gli obblighi di non divulgazione e diffusione delle informazioni riservate sono previsti nel contratto individuale di lavoro per il personale interno e in apposite *Non Disclosure Agreement* (NDA) per i collaboratori e i fornitori esterni. Tali accordi vengono documentati e riesaminati periodicamente.

Tutti gli obblighi al segreto e alla riservatezza a cui sono tenuti i dipendenti e i collaboratori dell'Amministrazione Regionale rimangono in essere e validi anche dopo la cessazione del rapporto di lavoro o del rapporto di collaborazione .

3.7 Obbligo di condivisione ed informazione

Tutto il personale, a qualsiasi livello, e tutti i collaboratori hanno l'obbligo di comunicare al proprio responsabile e/o alla struttura competente in materia ICT, azioni, situazioni, rischi, procedure (internee/o esterne), stati di fatto, interazioni, attività o altro che possano comportare un rischio per la sicurezzae la riservatezza dei dati e delle informazioni.

3.8 Copia delle informazioni e gestione supporti strumentiportatili

La copia dei dati personali e di informazioni deve essere effettuata con modalità che ne garantiscano la sicurezza e secondo criteri di assoluta necessità.

L'Amministrazione Regionale mette a disposizione una struttura di "repository" ovvero di "magazzino"per le informazioni e per i dati tale per cui ne siano garantite:

- riservatezza (garanzia che le informazioni siano accessibili solo da parte delle persone autorizzate);
- integrità (salvaguardia dell'accuratezza e della completezza);
- disponibilità (garanzia che gli utenti autorizzati abbiano accesso alle informazioni ed alle risorse associate solo quando ne hanno bisogno).

La copia di un'informazione con modalità diverse da quelle indicate nel presente atto, in quanto espongono l'amministrazione regionale a un considerevole rischio per la sicurezza dei dati e delle informazioni (per esempio accesso alle informazioni contenute in Pen Drive, HD esterni, file salvati inlocale sui PC, anche in caso di formattazione semplice da parte di un esperto del settore), è consentitasolo in via residuale e in assenza di soluzioni tecniche alternative perseguibili, e nel rispetto delle seguenti regole di condotta:

1) è vietato di copiare, trasferire, o muovere file dai server o NAS (Network Access Storage) interne su PC portatili o supporti removibili, tranne che per esigenze eccezionali e solo se espressamente autorizzato da figure dotate degli opportuni poteri amministrativi (in tal caso, l'autorizzazione deve essere accompagnata da indicazioni utili per la sicurezza delle informazioni);
2) non appena cessate tali esigenze, i file devono essere ritrasferiti sui server dell'Amministrazione Regionale, eliminandoli dal dispositivo portatile;
3) la memorizzazione dei dati sulle Pen Drive deve essere esclusivamente a carattere temporaneo (possibilmente nell'ordine di poche ore) e le stesse debbono essere oggetto di formattazione immediata dopo l'utilizzo temporaneo del file memorizzato. Le Pen Drive devono essere tassativamente rilasciate senza alcun file al loro interno;
4) è fatto comunque divieto di utilizzare supporti rimovibili personali;
5) non lasciare mai incustodito un dispositivo portatile, in particolare non lasciare mai sulla scrivania, rendendoli facilmente accessibili, pen drive o HD esterni. Gli stessi debbono esserecustoditi in cassetti o armadi chiusi a chiave e comunque gestiti con la stessa accortezza e diligenza delle altre risorse in dotazione;
6) deve essere sempre applicata la policy del "*bring the device always with you*", ovvero non lasciare incustodito un dispositivo, nell'automobile, presso soggetti esterni in area noncontrollata, in sale riunioni non chiuse a chiave, ecc. ;

7) non trascrivere informazioni sensibili (login, password, ecc.), né in forma cartacea né in forma elettronica, all'interno di un dispositivo, a meno che questo non avvenga mediante opportunaprocedura di crittazione dei dati precedentemente autorizzata e concordata con la dirigenza e/o la struttura competente in materia ICT;
8) per i medesimi motivi, lo scambio di informazioni e/o di dati anche all'interno dell'organizzazione dovrebbe avvenire mediante condivisione della risorsa all'interno dei server e/o delle NAS interne, piuttosto che per posta elettronica e/o mediante l'uso di dispositivi removibili;
9) non usare dispositivi come Pen Drive per il salvataggio primario di file ovvero per l'editing online invece di usare i supporti interni al PC.

3.9 Politica del "Clean Desk" e "Clean Desktop"

I Collaboratori, nello svolgimento della propria attività devono uniformarsi a politiche di "Clean Desk" e "Clean Desktop" in particolare attraverso l'osservanza delle seguenti regole ed obblighi.

3.9.1 Regole di condotta per l'applicazione della politica di "CleanDesk" e "Clean Desktop"

E' vietato:

1) lasciare documenti cartacei visibili sulla scrivania e sul posto di lavoro anche in assenza del titolare o del "custode" dei documenti stessi;
2) stampare e lasciare stampe e documenti cartacei incustoditi e al di fuori del proprio ufficio o luogo di lavoro, senza comunque proteggere le informazioni ivi contenute;
3) lasciare incustoditi, nel proprio ufficio o luogo di lavoro e/o anche al di fuori di questi, supportidi memorizzazione che contengono dati o informazioni dell'organizzazione (CDROM DVD, Pen Drive, HD esterni, memorie SD ecc. ecc. ;
4) lasciare incustoditi file o documenti cartacei che riportino informazioni altamente riservate come password o criteri di accesso ai sistemi;
5) lasciare la propria postazione attiva senza un blocco logico in modo che nessuna possa operare sulla sessione di lavoro aperta;
6) tenere copie di documenti sul proprio desktop del PC che non siano strettamente necessari alla fase di modifica;
7) fare eccessive copie di file e documenti, perdendo completamente la gestione delle revisionie rendendo impossibile sapere se un documento è quello in corso o meno;
8) limitare l'utilizzo di scannerizzazioni o copie di documenti critici e/o ad alto rischio od impattosulla sicurezza complessiva.

Le informazioni critiche, per esempio su carta o su supporti di memorizzazione digitale, quando non utilizzate, devono essere custodite chiuse a chiave (in cassaforte o armadio o altri mobili con caratteristiche di sicurezza) in particolare in caso di assenza dal proprio ufficio o luogo di lavoro.

3.9.2 Obblighi specifici per l'applicazione della politica di "CleanDesk" e "Clean Desktop"

1) I computer e terminali non debbono essere lasciati collegati o questi devono essere protetti, quando incustoditi, con un salva-schermo e meccanismi di blocco della tastiera controllati conuna password o token o con altri meccanismi similari di autenticazione dell'utente.
2) Le stampe contenenti informazioni riservate o classificate devono essere rimosse immediatamente dalle stampanti.
3) Tutti i computer workstation devono essere bloccati quando l'area di lavoro non è occupata.
4) Tutti i computer workstation devono essere spenti al termine della giornata lavorativa. Nel caso in cui dati ed alle informazioni trattati nella sessione di lavoro abbaino particolare impattosulla sicurezza e la riservatezza, il computer dovrà essere spento anche durante la giornatase la postazione di lavoro non viene usata per due ore o più.
5) Quando la scrivania non è presidiata ed alla fine della giornata di lavoro i documenti devono essere rimossi dalla scrivania ed riposti in un cassetto o altro luogo chiuso a chiave.
6) Gli armadi contenenti dati personali ed informazioni riservate devono essere mantenuti chiusie bloccati quando non sono in uso e non sono presidiati a vista.
7) Strumenti di accesso quali chiavi digitali, token, smart card, ecc. ecc. (utilizzati per accedere a informazioni riservate o ristrette) non devono essere mai lasciati incustoditi.
8) Computer portatili devono essere bloccati con un cavo anti effrazione o chiusi a chiave in cassetti o armadi.
9) Il login e la password sono informazioni strettamente riservate che dovranno essere memorizzate, senza trascriverli e mantenerli visibili tramite post-it o altre modalità nella postazione di lavoro e/o in una posizione comunque facilmente accessibile.
10) Nel caso di stampa di documenti contenenti dati personali e informazioni riservate gli stessidevono essere immediatamente rimosse dalla stampante.
11) I documenti riservati e/o ad accesso limitato, non più necessari, devono essere distrutti nel distruggi documenti e non lasciati senza protezione
12) Lavagne contenenti informazioni devono essere cancellate ed i fogli distrutti.
13) Bloccare immediatamente i dispositivi informatici portatili come i laptop e tablet subito dopo illoro uso, anche per assenze temporanee molto brevi.
14) Trattare i dispositivi di archiviazione di massa come CD-ROM, DVD, o unità USB / Pen Drivecome critici e chiuderli sempre in un cassetto o armadio.
15) Identificare sempre le Pen Drive utilizzate, in modo che un loro furto possa essere sempre identificato.

3.10 Navigazione Internet

È vietata la navigazione sulla rete internet per scopi diversi da quelli strettamente legati all'attività lavorativa, sia attraverso le Risorse ICT, sia attraverso connessioni Internet personali.

E' vietato scaricare da siti internet software *freeware* e *shareware* , file musicali e video.

Non è consentita la partecipazione a Forum non professionali, l'utilizzo di chat line, bachecheelettroniche, blog e la registrazione su "*guest book*", anche utilizzando "*nick name*".

L'ascolto di file audio e la visione di file video sono consentiti, solo se autorizzati dal dirigente per

motivi attinenti all'attività lavorativa.

Le precedenti disposizioni debbono essere osservate anche per l'utilizzo di "app" installate susmartphone, tablet e smartwatch, che, per il loro funzionamento, accedano alla rete ICT interna.

L'Amministrazione regionale, al fine di evitare la navigazione su siti web non pertinenti all'attività lavorativa, si riserva la facoltà di inserire un blocco e/o un filtro automatico in grado di impedire l'accesso a determinati siti web che saranno indicati in una "*blacklist*", ovvero ai contenuti o alla classificazione dei siti web consultati.

Le precedenti disposizioni e i predetti divieti trovano applicazione, per quanto possibile, anche all'utilizzo di dispositivi personali durante l'orario di lavoro e ferma ogni altra disposizione di legge in materia.

3.11 Uso di dispositivi personali

3.11.1 Collegamento a rete Wi-Fi pubblica

In conformità con l'art. 8-bis "Connettività alla rete Internet negli uffici e luoghi pubblici" del Decreto Legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" e sue modificazioni, Regione Marche ha creato una rete ad accesso libero per ospiti (guest).

L'utilizzatore può collegarsi in maniera automatica per la sola navigazione Internet alla rete Wi-Fi . Al primo collegamento il sistema invia all'utente un codice di attivazione via SMS tramite il quale è possibile l'accesso alla rete. Al fine di preservare la sicurezza della rete interna da questa tipologia diaccessi, le due reti restano completamente separate.

3.11.2 Collegamento a rete ICT interna

Il Collaboratore può collegare un suo dispositivo, anche mobile (come lo smartphone) alla rete internasolo a seguito di una esplicita autorizzazione della funzione ICT.

Nel caso in cui gli utenti abbiano configurato posta elettronica e altre app fornite dall'ente sui propri supporti mobili (smartphone, tablet ecc.), dovranno obbligatoriamente proteggere l'accesso al dispositivo con credenziali o PIN ed installare un sistema antivirus aggiornato.

3.12 Utilizzo della posta elettronica e messaggistica

I Collaboratori assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo dellestesse. Pertanto è fatto divieto di utilizzare le caselle di posta elettronica facenti riferimento al dominio dell'Amministrazione Regionale o in qualche modo alla stessa riconducibile, per l'invio di messaggi a interlocutori personali e/o con contenuti non strettamente necessari per l'attività professionale

E' vietato l'invio di posta elettronica da persona diversa da quella che riveste i poteri per effettuare la comunicazione medesima, ossia colui che ha effettuato l'accesso al sistema mediante il login e password assegnatigli.

Ai collaboratori esterni non viene assegnata una casella di posta a dominio dell'Amministrazione Regionale, salvo che venga specificatamente richiesto dal dirigente o da altro organo competente.

Non è consentito diffondere messaggi di posta elettronica a diffusione capillare e moltiplicata.

L'iscrizione a *mailing list* esterne è cosentita solo per ragioni lavorative, previa verifica, prima dell'iscrizione, dell'affidabilità del sito ospitante, con il supporto della struttura competente in materia ICT.

Non è consentito l'utilizzo delle mailing list regionali per comunicazioni non strettamente attinenti all'attività lavorativa o istituzionale o concernenti il ruolo ricoperto all'interno dell'amministrazione regionale.

E' severamente vietato qualsiasi utilizzo delle mailing liste regionali per l'invio di comunicazioni personali, commerciali o a carattere pubblicitario.

I rappresentati sindacali possono utilizzare le mailing list ai sensi dell'art.25 della legge 300/70 al fine della diffusione di pubblicazioni, testi, e comunicati inerenti materie di interesse sindacale.(DGR 1394/08)

In caso di necessità di utilizzo di sistemi di messaggistica quali ad esempio Skype, Msn, Telegram, Whatsapp, ecc., lo stesso dovrà essere concordato con i tecnici della struttura competente in materia ICT per le valutazioni tecniche del caso.

In caso di assenze programmate, il collaboratore dovrà impostare la funzione di risposta automatica per la propria casella di posta interna, fornendo nel messaggio tutte le indicazioni utili alla corretta prosecuzione dell'attività lavorativa in sua assenza e, in particolare, il recapito mail del proprio sostitutopro tempore e, se necessario , del proprio diretto superiore gerarchico.

In caso di assenze non programmate, l'impostazione della funzione di risposta automatica deve essere comunque attivata entro 24 ore dal collaboratore stesso.

In caso di mancata attivazione, l'Amministrazione regionale si riserva la facoltà di provvedere a tale incombenza mediante l'intervento della sua struttura competente in materia ICT, anche modificando temporaneamente la password di accesso.

Di tale intervento viene data immediata comunicazione al Collaboratore interessato.

4 Disposizioni finali

La presente policy è vincolante per tutti i collaboratori dell'Ente regionale.

E' applicabile anche agli organi di indirizzo politico che utilizzano strumenti informatici dell'Amministrazione Regionale, fatta eccezione per le disposizioni sanzionatorie e disciplinari.

La stessa viene consegnata in formato cartaceo o comunicata in formato digitale ai dipendenti dell'ente, al momento dell'assunzione, e comunicata ai collaboratori esterni e/o ai dipendenti di fornitori, al momento dell'instaurazione del rapporto contrattuale.

La presente policy deve anche essere comunicata ai dipendenti e collaboratori che siano già registrati sui sistemi informativi interni al momento della sua entrata in vigore.

Ai fini della sua piena conoscibilità da parte di tutti gli interessati, la presente policy viene anche pubblicata sulla sezione "Sicurezza informatica" della pagina intranet dell'Ente.