Allegato 1

REGOLAMENTO IN MATERIA DI TELELAVORO (O LAVORO DA REMOTO)

ART. 1
DEFINIZIONE

1. Il telelavoro (o lavoro da remoto) è finalizzato a introdurre soluzioni organizzative atte a promuovere la conciliazione dei tempi di vita e di lavoro dei dipendenti dell'Agenzia Regionale Sanitaria, attraverso una modificazione del luogo di adempimento della prestazione lavorativa, che comporta la effettuazione della stessa in uno spazio idoneo e diverso dalla sede dell'ufficio al quale il dipendente è assegnato,nel rispetto dell'orario di lavoro giornaliero.
2. Il telelavoro si realizza all'interno del preesistente rapporto di lavoro; rimangono invariate la struttura di assegnazione e l'inquadramento del dipendente.
3. Il telelavoro è alternativo e non cumulabile con lo smart working di cui all'art. 18 della L. 22 maggio 2017, n. 81, dal quale si differenzia, oltre che per le finalità a cui risponde, anche per i seguenti aspetti:
    a. il luogo di lavoro diverso dalla sede dell'ufficio è individuato in maniera fissa nel progetto di telelavoro ed è soggetto da parte dell'amministrazione a verifica di conformità alle norme generali di prevenzione e sicurezza;
    b. il dipendente in telelavoro è soggetto ai medesimi obblighi derivanti dal lavoro prestato in sede con particolare riferimento al rispetto delle disposizioni in materia di orario di lavoro, inclusi obblighi e diritti legati a riposi, pause, permessi orari;
    c. nel telelavoro, la fornitura della postazione di lavoro completa, comprensiva di mobilio, è a carico dell'amministrazione che la concede in comodato d'uso gratuito per la durata del progetto.

ART. 2
FINALITA'

1. L'Agenzia Regionale Sanitaria ricorre al telelavoro al fine di:

    a. favorire l'integrazione lavorativa dei dipendenti nel caso in cui, per cause dovute a condizioni di disabilità o altri impedimenti di natura oggettiva, personali o familiari, anche transitori, risulti particolarmente gravoso lo spostamento casa-lavoro e viceversa;

    b. incrementare il benessere organizzativo, promuovendo in contemporanea la mobilità sostenibile nell'ottica di una politica ambientale sensibile alla diminuzione del traffico urbano.

2. Come previsto dall'art. 6, comma 4, dell'Intesa sullo schema di linee guida in materia di lavoro agile del 16 dicembre 2021, l'Amministrazione può adottare il lavoro da remoto, anche nel caso di attività, previamente individuate dalla stessa, "*ove è richiesto un presidio costante del processo e ove sussistono i requisiti tecnologici che consentano la continua operatività ed il costante accesso alle procedure di lavoro ed ai sistemi informativi oltreché affidabili controlli automatizzati sul rispetto degli obblighi derivanti dalle disposizioni in materia di orario di lavoro*".

ART. 3
TIPOLOGIE DI TELELAVORO

1. Le tipologie di lavoro da remoto attuabili sono:

a) *telelavoro domiciliare*, che comporta la prestazione dell'attività lavorativa dal domicilio del dipendente:

I - telelavoro domiciliare annuale: rientrano in questa tipologia i progetti di telelavoro attivati in relazione ad esigenze di conciliazione vita-lavoro legate, in particolare, all'organizzazione familiare, specialmente se determinate dalla presenza di minori o anziani all'interno del nucleo familiare. In apposito atto di pianificazione annuale, viene stabilito il numero massimo dei posti a disposizione per tale casistica nell'ambito della percentuale di cui all'articolo 5, comma 1;

II - telelavoro domiciliare per esigenze straordinarie: rientrano in questa tipologia i progetti di telelavoro domiciliare attivati in relazione al riconoscimento di situazioni di handicap grave del dipendente ai sensi dell'art. 3, c. 3 della legge 104/92 o di patologie gravi dello stesso che richiedano terapie salvavita ed altre assimilabili come stabilito dalle normative contrattuali. Ai sensi dell'art. 37, c. 2 del CCNL 21 maggio 2018, "*l'attestazione della sussistenza delle particolari patologie richiedenti le terapie salvavita di cui al comma 1 deve essere rilasciata dalle competenti strutture medico-legali delle Aziende sanitarie locali o dalle strutture con competenze mediche delle pubbliche amministrazioni o da enti accreditati*". Questa tipologia di telelavoro ha durata coincidente con quella della causa che ne giustifica il riconoscimento. In ogni caso è necessario comunicare annualmente alla struttura competente in materia di personale il permanere della causa che ne ha giustificato il riconoscimento.

III - telelavoro domiciliare per esigenze temporanee e/o imprevedibili: in caso di documentate esigenze familiari o personali a carattere temporaneo e/o imprevedibile, di durata superiore a un mese e presumibilmente inferiore a 6 mesi, è possibile adibire il dipendente a telelavoro – anche senza fornitura dell'intera strumentazione – qualora lo stesso sia in condizioni di lavorare e quando l'assenza potrebbe determinare significativi ritardi dell'attività dell'amministrazione;

b) *altra forma di lavoro a distanza* da "*centri satellite*" con benefici in termini di conciliazione dei tempi di vita-lavoro*; i centri satellite* possono essere dislocati presso:

   a. le sedi decentrate territoriali della Giunta regionale, acquisito l'assenso del dirigente della struttura dirigenziale ospitante;
   b. le sedi di altri enti pubblici presenti sul territorio regionale, valutati l'interesse e l'economicità della soluzione proposta, *previa stipula di apposita convenzione*;
   c. le sedi di soggetti privati site nel territorio regionale, valutati l'interesse e l'economicità della soluzione proposta, *previa stipula di apposita convenzione*.

ART. 4
ATTIVITA' TELELAVORABILI

1. Per attività telelavorabili si intendono le singole attività, tra quelle alle quali è adibito ciascun dipendente, che possono essere gestite al di fuori del luogo di lavoro dove normalmente vengono svolte, quali risultanti nel documento "*Mappatura delle attività*" disponibile nella sotto Sezione dell'Amministrazione Trasparente "*Atti Generali*", e/o dal decreto annuale delle linee di attività redatto da ciascun responsabile di struttura dirigenziale
2. Un'attività è telelavorabile quando:

a) l'attività riguarda la creazione, l'elaborazione e trasmissione di informazioni, dati,documentazione e si svolge con un elevato grado di autonomia;

b) l'attività non prevede il contatto personale diretto con l'utenza presso un ufficio o uno sportello ovvero rapporti con interlocutori che non possano essere gestiti con efficacia attraverso strumenti telematici e/o concentrati nei giorni di presenza effettiva in ufficio;

c) l'attività non richiede incontri e riunioni frequenti con i colleghi, anche di altre strutture dirigenziali, o prevede riunioni efficacemente gestibili tramite piattaforme telematiche;

d) la prestazione è chiaramente definita e gli obiettivi assegnati ben identificabili e misurabili quanto al loro raggiungimento.

ART. 5
ACCESSO AL TELELAVORO DOMICILIARE ANNUALE E PRESSO CENTRI SATELLITE

1. Entro il 31 gennaio di ogni anno, viene predisposto apposito piano annuale per l'utilizzo del telelavoro con indicazione del numero di postazioni di telelavoro domiciliari e satellitari disponibili nel limite massimo del 5% del personale del comparto a tempo indeterminato. Le casistiche di telelavoro di cui all'art. 3, comma 1, lett. a), punti II e III non sono ricomprese nella percentuale di cuial periodo precedente.
2. Entro il 28 febbraio di ciascun anno viene pubblicato un avviso per individuare i dipendenti da avviare al telelavoro.
3. Possono presentare domanda di telelavoro i dipendenti del comparto in servizio a tempo indeterminato, con orario di lavoro a tempo pieno o parziale, qualora svolgano attività telelavorabili ai sensi del precedente art. 4.
4. Il Settore Affari Generali dell'ARS effettua un'istruttoria delle richieste pervenute in risposta all'avviso con le modalità previste al successivo articolo 7.
5. Nel caso in cui le richieste superino il numero di posti disponibili, viene predisposta una graduatoria, nel rispetto dei seguenti criteri di precedenza definiti in coerenza con l'art. 4 dell'Accordo quadro del 23 marzo 2000 e con il presente regolamento:
   a) dipendente con patologie croniche con scarso compenso clinico e con particolare connotazione di gravità, riconducibile alle casistiche di cui al DM 4 febbraio 2022;
   b) dipendente con handicap accertato ai sensi dell'art. 4 e con le caratteristiche di cui all'art. 3, comma 1 della legge 104/92;
   c) dipendente in situazione di gravità psicofisica ancorché non accertata ai sensi della legge 104/92, ma certificata da struttura pubblica competente;
   d) assistenza a conviventi con grave handicap accertato ai sensi dell'art. 4 e con le caratteristiche di cui all'art. 3, comma 3 della legge 104/92;
   e) assistenza ai parenti o affini, anche non conviventi, entro il secondo grado o entro il terzo nei casi di cui all'art. 33 della legge 5 febbraio 1992 n. 104 con grave handicap accertato, ai sensi dell'art. 4 e con le caratteristiche di cui all'art. 3, comma 3 della legge 104/92;
   f) assistenza a conviventi con handicap accertato ai sensi dell'art. 4 e con le caratteristiche di cui all'art. 3, comma 1 della legge 104/92;
   g) assistenza ai parenti o affini, anche non conviventi, entro il secondo grado o entro il terzo nei casi di cui all'art. 33 della legge 5 febbraio 1992 n. 104 con handicap accertato, ai sensi dell'art. 4 e con le caratteristiche di cui all'art. 3, comma 1 della legge 104/92;

h) assistenza a parenti o affini fino al terzo grado conviventi in situazione di gravità psicofisica ancorché non accertata ai sensi della legge 104/92, ma certificata da struttura pubblica competente;
i) assistenza a parenti o affini fino al terzo grado anche non conviventi nei casi di cui all'art. 33 della legge 5 febbraio 1992 n. 104 in situazione di gravità psicofisica ancorché non accertata ai sensi della legge 104/92, ma certificata da struttura pubblica competente;
j) organizzazione familiare con riferimento all'età del minore fino a 3 anni compiuti;
k) organizzazione familiare con riferimento all'età del minore fino a 8 anni compiuti;
l) organizzazione familiare con riferimento all'età del minore fino a 12 anni compiuti;
m) difficoltà di raggiungimento della sede di lavoro dal proprio domicilio, in termini di distanza kilometrica quale risultante da Google Maps o strumenti analoghi;
n) difficoltà di ricongiungimento familiare dovute alla lontananza della sede di lavoro del coniuge/convivente dal domicilio che impedisca il ricongiungimento familiare quotidiano.

6. Per il criterio relativo alla distanza kilometrica, viene riconosciuta una maggiore priorità, in corrispondenza di una maggiore distanza.
7. A seguito dell'applicazione dei suddetti criteri di precedenza, in caso di parità, si privilegia il dipendente di età anagrafica maggiore.
8. Il dirigente della struttura competente in materia di personale adotta con decreto la graduatoria e la comunica agli interessati.

ART. 6
ACCESSO AL TELELAVORO DOMICILIARE PER ESIGENZE STRAORDINARIE E PER ESIGENZE TEMPORANEE E/O IMPREVEDIBILI

1. Le richieste di accesso al telelavoro domiciliare per esigenze straordinarie o temporanee e/o imprevedibili quali definite al precedente articolo 3 possono essere inoltrate dal personale interessato in qualsiasi periodo dell'anno, al verificarsi di una delle condizioni che le giustificano.
2. Il personale interessato presenta, con un anticipo adeguato rispetto alla decorrenza e comunque non inferiore a 10 giorni, una proposta di progetto redatta congiuntamente con il responsabile della struttura di appartenenza, come al successivo articolo 7, da corredare con la documentazione comprovante le specifiche esigenze.
3. La struttura competente in materia di personale effettua l'istruttoria delle domande pervenute e provvede alla validazione.
4. Le tipologie di telelavoro di cui al comma 1 del presente articolo possono essere richieste anche dal personale dirigenziale e dal personale a tempo determinato.

ART. 7
MODALITA' DI ATTIVAZIONE DEL TELELAVORO

1. L'attuazione delle forme di telelavoro domiciliare o da centro satellite avviene attraverso la predisposizione del progetto mediante apposito giustificativo di Cohesion come da allegato A, previa autorizzazione del dirigente. Ai fini dell'efficacia del progetto, la presentazione della domanda da parte del dipendente e la validazione da parte del dirigente costituiscono sottoscrizione.
2. Gli adempimenti procedurali necessari per l'attivazione del telelavoro sono:
   - compilazione della proposta di progetto mediante giustificativo Cohesion;
   - autorizzazione del giustificativo da parte del dirigente responsabile;
   - istruttoria da parte del Settore Affari Generali dell'ARS;

- "allestimento" della postazione (attrezzature hardware e software, eventuale tavolo, poltrona ergonomica, e/o altro mobilio necessario) come definita al successivo articolo 10 e verifiche – di norma da remoto e in modalità digitale - di idoneità del locale, ai fini della conformità alle vigenti norme in materia di ambiente, salute e sicurezza sul lavoro;
- validazione da parte della struttura responsabile in materia di personale.

3. La decorrenza del progetto di telelavoro inizia il primo giorno del mese successivo a quello in cui è avvenuta la validazione da parte del Settore Affari Generali.
4. Per i soli progetti di telelavoro domiciliare per esigenze straordinarie o per esigenze temporanee e/o imprevedibili la decorrenza inizia dal giorno successivo alla data di validazione da parte del Settore Affari Generali.

ART. 8
DISPOSIZIONI RELATIVE AL RAPPORTO DI LAVORO

1. L'assegnazione a progetti di telelavoro non muta la natura del rapporto di lavoro subordinato in atto; vengono pertanto, garantiti gli istituti previsti dalla contrattazione collettiva nazionale integrativa e decentrata tenendo conto della specialità della prestazione in modalità telelavoro.
2. Il telelavoratore domiciliare o dislocato presso centro satellite in locali non nella disponibilità della Giunta regionale, presenta su base settimanale, apposita dichiarazione sostitutiva ai sensi dell'articolo 47 del DPR n. 445 del 2000 circa l'orario di lavoro prestato. La dichiarazione, firmata digitalmente o in forma autografa, va trasmessa al proprio operatore presenze e al dirigente responsabile.
3. Previo accordo con il dirigente responsabile, vengono individuati due periodi di un'ora nell'arco della giornata in cui il dipendente è disponibile per comunicazioni da parte dell'amministrazione.
4. Il telelavoro viene svolto di norma fino a un massimo di 4 giornate alla settimana prevedendo almeno un giorno di presenza in sede. In caso di telelavoro per esigenze "temporanee e/o imprevedibili" di cui all'art. 3 c. 1 lett. a), punto III, il dirigente e il dipendente possono concordare modalità di rientro diverse.
5. Il dipendente che presta la propria attività in telelavoro da centro satellite coincidente con una sede della Giunta regionale non è tenuto ad alcun rientro presso la sede ordinaria – salvo diversa valutazione del dirigente da indicare nel progetto di telelavoro - ed effettua le timbrature nei terminali non presente nella sede ospitante.
6. Durante le giornate in telelavoro domiciliare non sono configurabili prestazioni aggiuntive, straordinarie, notturne o festive, sono invece garantiti i riposi, le pause e permessi orari.
7. Il telelavoratore domiciliare non ha diritto al buono pasto la cui erogazione è prevista solo nei giorni di rientro obbligatorio presso la sede di lavoro, secondo quanto stabilito dalla disciplina dell'orario di lavoro dell'Ente.
8. Non è previsto il rimborso delle spese di trasporto né di missione per gli accessi presso la sede della struttura di appartenenza nei giorni determinati nel progetto.
9. Ai dipendenti in telelavoro è garantita, alla condizione del rientro in sede, la partecipazione ai corsi di formazione in presenza diretti ai dipendenti regionali, attinenti all'attività svolta e concordati con il dirigente della struttura di appartenenza. È garantita altresì al dipendente il livello di informazione e comunicazione istituzionali previsto per tutto il personale regionale.
10. È garantito l'esercizio dei diritti sindacali. Il lavoratore deve essere informato e deve poter partecipare all'attività sindacale dell'amministrazione come previsto dalla contrattazione vigente.
11. Il lavoratore ha il dovere della riservatezza su tutte le informazioni delle quali venga in possesso per il lavoro assegnategli e di quelle derivanti dall'utilizzo delle apparecchiature, dei programmi e dei

dati in essi contenuti. In nessun caso il lavoratore può eseguire lavori per conto proprio o per terzi utilizzando le attrezzature assegnategli senza previa autorizzazione dell'ente.

12. Per gli aspetti giuridici ed economici non espressamente richiamati dal presente articolo resta confermata la disciplina contenuta contrattazione collettiva vigente.
13. Il dipendente che presta la propria attività in telelavoro è tenuto a trasmettere al proprio dirigente un report quindicinale firmato digitalmente o in forma autografa con l'indicazione delle attività svolte nel periodo di riferimento.

ART. 9
INTERRUZIONE E REVOCA

1. Durante l'esecuzione del progetto, l'amministrazione può comunicare al dipendente, previa motivazione, la necessità di interruzione dello stesso, con la garanzia di un preavviso di almeno 30 giorni.
2. Il dipendente addetto al telelavoro può presentare per iscritto all'amministrazione di appartenenza una richiesta motivata di reintegrazione nell'ordinario rapporto di lavoro, non prima che sianotrascorsi sei mesi dall'avvio del progetto; tale termine può essere derogato solo in presenza di gravi e comprovati motivi personali sopravvenuti, che rendano impossibile proseguire l'esperienza di telelavoro.

ART. 10
POSTAZIONE DI TELELAVORO

1. Per postazione di telelavoro si intende la necessaria attrezzatura tecnologica (hardware e software) ed eventuale mobilio (scrivania, sedia, ecc.), qualora necessari.
2. L'amministrazione concorda con il lavoratore il luogo ove viene prestata l'attività lavorativa ed è tenuta alla verifica della sua idoneità, anche ai fini della valutazione del rischio di infortuni, nella fasedi avvio e, successivamente, con frequenza almeno semestrale. Nel caso di telelavoro domiciliare, concorda con il lavoratore tempi e modalità di accesso al domicilio per effettuare la suddetta verifica.
3. Il lavoro da remoto viene realizzato, di norma, con l'ausilio di dispositivi tecnologici, messi a disposizione dall'amministrazione in comodato, che ne garantisce anche la manutenzione e la gestione dei sistemi di supporto.
4. La strumentazione ed i collegamenti necessari per la postazione di telelavoro secondo il più aggiornato standard tecnologico è a cura dell'Amministrazione.
5. Qualsiasi guasto dovuto all'attrezzatura tecnologica deve essere subito segnalato dal telelavoratore all'amministrazione, la quale, qualora il guasto non sia riparabile in tempi ragionevoli, ha la facoltà di ordinare il rientro del telelavoratore per il periodo necessario al ripristino del sistema.
6. Per i progetti di telelavoro domiciliare annuale e per esigenze straordinarie il lavoratore utilizza il proprio collegamento internet e l'amministrazione gli corrisponde un rimborso forfettario annuale pari a 50 euro.
7. Per i progetti di telelavoro domiciliare annuale e per esigenze straordinarie, l'amministrazione corrisponde al lavoratore una somma a titolo di rimborso dei consumi energetici (luce e gas), pari a 1/3 delle spese sostenute fino al tetto massimo di 300 euro annui (per l'ipotesi di quattro giornate di telelavoro, da riproporzionarsi in caso di un minor numero di giornate telelavorate).
8. I rimborsi sono erogati normalmente in occasione del pagamento dello stipendio di novembre.

9. La postazione di lavoro può essere utilizzata esclusivamente per le attività inerenti al rapporto di lavoro.
10. Fermo restando la copertura INAIL in caso di infortuni come per i dipendenti che lavorano in sede, l'amministrazione stipula polizze assicurative per la copertura dei seguenti rischi:
    a. Danni alle attrezzature in dotazione, con esclusione di quelli derivanti da dolo o colpa grave;
    b. Danni a cose o persone, compresi i familiari del dipendente derivanti dall'uso delle attrezzature.

ART. 11
SICUREZZA PREVENZIONE E PROTEZIONE

1. Nel lavoro da remoto, il dipendente deve attenersi a tutte le norme e regolamenti in vigore, nonché prestare la dovuta attenzione per evitare che si producano situazioni pericolose o si verifichino infortuni.

2. Il dipendente è tenuto ad utilizzare la postazione di telelavoro esclusivamente per motivi inerenti il lavoro, a rispettare le norme di sicurezza, incluse gli allegati 1 e 2 al presente regolamento rispettivamente denominati "Salute e sicurezza del personale" e "Policy per la sicurezza informatica e per l'utilizzo degli strumenti informativi e telematici". Il dipendente si impegna altresì a non manomettere in alcun modo le apparecchiature, a non variare la configurazione della postazione, a non sostituirla con altre apparecchiature o dispositivi tecnologici, a non utilizzare collegamenti alternativi o complementari.

3. Nel telelavoro domiciliare la disponibilità, nell'abitazione del lavoratore interessato, di un ambiente o uno spazio di lavoro dedicato all'attività nel rispetto delle norme in materia di sicurezza e salute dei lavoratori, è condizione necessaria per l'autorizzazione; il dipendente deve presentare certificazione di conformità dell'impianto elettrico per i locali destinati alla postazione di lavoro.

4. Al fine di verificare la corretta applicazione delle norme in materia di salute e sicurezza, l'Amministrazione e le autorità competenti ove necessario, hanno accesso al luogo in cui viene svolto il telelavoro; ove il telelavoratore svolga l'attività nel proprio domicilio, tale accesso è subordinato a preavviso e al consenso come prestato all'interno del progetto di telelavoro.

ART. 12
VERIFICA PRESTAZIONI

1. La metodologia di lavoro comporta una valutazione delle prestazioni del lavoratore orientata ai risultati. Il sistema di valutazione esistente è adeguato e tale da garantire la parità di trattamento con i dipendenti che operano in sede.
2. Fermo restando che nessun dispositivo di controllo può essere attivato all'insaputa dei lavoratori, la verifica dell'adempimento della prestazione viene effettuata dal dirigente a cui il dipendente è assegnato.
3. Nel progetto di telelavoro vengono definiti i risultati da raggiungere da parte del dipendente; il dirigente verifica l'andamento dell'attività in telelavoro, in riferimento agli obiettivi annuali di performance individuali e organizzativi.
4. Qualora dalle verifiche effettuate dovesse emergere che il dipendente non ha provveduto all'esecuzione dei compiti assegnati per cause allo stesso imputabili, sarà cura del dirigente, interrompere il progetto di telelavoro o per la valutazione di eventuali sanzioni.

5. Resta ferma la possibilità che il dirigente accerti direttamente le condizioni che giustificano i provvedimenti di cui al periodo precedente.

ART. 13
MONITORAGGIO ED EFFETTI DEL TELELAVORO

1. Sulla base dei dati a disposizione o previa somministrazione di appositi questionari, il Settore Affari Generali attiva un monitoraggio al fine di verificare il raggiungimento dei seguenti obiettivi:
   - favorire il miglioramento del clima lavorativo (miglioramento dei rapporti interpersonali, della motivazione, del senso di appartenenza; diminuzione dell'ansia e dello stress) anche attraverso il BOM (Benessere Organizzativo Marche);
   - favorire il rientro dal part-time o l'aumento della base oraria del personale part-time;
   - favorire il rientro dalla maternità in tempi più brevi e/o la riduzione del numero di giorni richiesti per congedi e/o aspettative.

ART. 14
TRASPARENZA

1. Il Piano annuale e il numero delle procedure di telelavoro domiciliari attivate sono pubblicati sul sito istituzionale dell'Agenzia Regionale Sanitaria – Amministrazione Trasparente – Altri contenuti – Accessibilità e Catalogo dati, metadati e banche dati.

ART.15
CLAUSOLE DI TUTELA

1. Per tutto quanto non espressamente previsto nel presente regolamento si fa riferimento alle leggi vigenti, al CCNL funzioni locali e agli accordi integrativi.
2. L'assegnazione a progetti di telelavoro deve consentire al lavoratore pari opportunità, quanto a possibilità di carriera, di partecipazione a iniziative formative e di socializzazione rispetto ai lavoratori che operano in sede.

Art. 16
DISPOSIZIONI SPECIALI E TRANSITORIE

1. Al fine di facilitare l'utilizzo di tale forma flessibile di svolgimento della prestazione lavorativa dei dipendenti dell'Agenzia Regionale Sanitaria, in presenza di calamità naturali, di stati di emergenza disposte con specifici provvedimenti straordinari statali o locali a tutela della salute o della sicurezza pubblica, potranno essere adottate dall'amministrazione specifiche misure derogatorie al presente regolamento.
2. Per l'anno 2023 la pubblicazione dell'avviso di cui all'art. 5, è prevista entro il 19 dicembre 2022 e comunque per il solo telelavoro domiciliare annuale.

3. In via di prima applicazione, i rapporti di telelavoro in corso inquadrati nell'art. 3, comma 1, lett. a) punto I, e riconducibili al punto b) restano efficaci fino alla data di attivazione dei nuovi progetti di telelavoro. Si fanno salvi comunque gli effetti dei progetti di telelavoro annuali autorizzati ai sensi della previgente disciplina fino alla loro naturale scadenza, per i dipendenti che non rientrino nella graduatoria approvata in esito al bando di cui all'art. 5 del presente regolamento.
4. I progetti di telelavoro domiciliare stabile già autorizzati ai sensi della disciplina previgente continuano a produrre effetti ai sensi della disciplina previgente fino al 28.02.2023. Le disposizioni di cui al presente regolamento si applicano a decorrere dal 1° gennaio 2023, a fronte della conferma del permanere delle condizioni che lo giustificano quali definite all'art. 3, comma 1, lett. a), punto II del presente regolamento.
5. I progetti di telelavoro domiciliare di emergenza già autorizzati ai sensi della disciplina previgente continuano a produrre effetti fino alla naturale scadenza alle condizioni precedentemente pattuite.
6. Per l'anno 2023 in relazione a quanto disposto dall'art. 3, comma 1, lett. b) del presente regolamento si stabilisce che, il telelavoro presso centri satellite dislocati sul territorio può essere svolto solo presso sedi dell'Agenzia Regionale Sanitaria.
7. Gli importi di cui ai commi 6 e 7 dell'art. 10 possono essere modificati in sede di contrattazione collettiva decentrata integrativa qualora nel tempo non risultino più congrui.

Allegato A1

INFORMATIVA
Tutela della Salute e della Sicurezza del personale in telelavoro

PRINCIPI GENERALI

Il/la lavoratore/trice che presta la propria attività lavorativa *da remoto*, 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).

E' dovere del/della lavoratore/trice mettere in atto ogni comportamento utile a limitare i rischi derivanti dall'esecuzione della prestazione lavorativa in telelavoro, 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:

- 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.

I luoghi di lavoro individuati dal/dalla lavoratore/trice per l'esecuzione della prestazione lavorativa nella modalità telelavoro devono rispettare le indicazioni previste per la sicurezza dei videoterminalisti.

Il/la lavoratore/trice 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 modalità telelavoro 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 sedileriguardano 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 inaltezza (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.

SEGNALAZIONE INFORTUNI

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

ALLEGATO 1

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 4
1.1 Definizioni 4
1.2 Riferimenti 4
1.3 Finalità 5
1.4 Ambito di applicazione 5
1.4.1 Rete ICT Interna 5
1.4.2 Strumenti ICT 5
2 Linee guida e misure tecniche ed organizzative 6
2.1 Figure e ruoli all'interno della Organizzazione Regionale 6
2.2 Sistema dei controlli 6
2.2.1 Gradualità 6
2.2.2 Controlli sui dispositivi in dotazione ai Collaboratori 7
2.2.3 Controlli per finalità tecniche e/o amministrative 7
2.2.4 Accesso da remoto 8
2.2.5 Log degli accessi 8
2.3 Proprietà degli strumenti / risorse informative 8
2.4 Regole generali in materia di domicilio informatico-digitale, identità digitale e posta elettronica 9
2.5 Cessazione dei servizi 10
2.6 Installazione ed utilizzo dei SoftWare 10
2.7 Protezione della rete telematica Regionale, della server farm e delle postazioni 11
2.7.1 Tutela riservatezza, integrità, disponibilità e resilienza della rete telematica – Backup 11
2.7.2 Amministratori di Sistema 11
2.7.3 Separazione dati anagrafici e particolari - pseudonimizzazione, cifratura, minimizzazione 12
2.7.4 Verifica adeguatezza al principio della "Privacy by design" 12
2.8 Disciplina dell'accesso alla rete telematica interna 12
2.8.1 Regole specifiche 12
2.8.2 Regole di accesso alla rete informatica 12
2.8.3 Regole di accesso alla rete fisica 13
2.8.4 Autenticazione tramite Cohesion 13

2.8.5 Regole di "Password Change" 13
2.8.6 Regole di disattivazione 14
3 Modalità di utilizzo dei sistemi e mezzi telematici da parte di dipendenti e collaboratori 14
3.1 Custodia delle risorse 14
3.2 Abuso e alterazione delle risorse ICT 15
3.3 Utilizzo condiviso delle risorse ICT 15
3.4 Cessazione del rapporto di lavoro 15
3.5 Obbligo alla riservatezza e al segreto professionale 16
3.6 Informazioni Riservate e Accordi di Riservatezza 16
3.7 Obbligo di condivisione ed informazione 17
3.8 Copia delle informazioni e gestione supporti strumenti portatili 17
3.9 Politica del "Clean Desk" e "Clean Desktop" 18
3.9.1 Regole di condotta per l'applicazione della politica di "Clean Desk" e "Clean Desktop" 18
3.9.2 Obblighi specifici per l'applicazione della politica di "Clean Desk" e "Clean Desktop" ... 19
3.10 Navigazione Internet 19
3.11 Uso di dispositivi personali 20
3.11.1 Collegamento a rete Wi-Fi pubblica 20
3.11.2 Collegamento a rete ICT interna 20
3.12 Utilizzo della posta elettronica e messaggistica 20
4 Disposizioni finali 21

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 lo più reperibile attraverso Internet.
Guest book	Libro degli ospiti inteso in informatica come un sito dove poter lasciare i propri 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'identità degli 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 registrazione utente su servizi on-line
SCCM	Sistema di gestione che consente di gestire un numero elevato di computer in esecuzione su vari sistemi operativi
Shareware	Software che può essere provato gratuitamente, pur rimanendo vincolato al 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 ricevere o 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 personali e 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 rischi e 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 atto è 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 Organizzazione Regionale

Sono individuate le seguenti figure interne all'organizzazione regionale alle quali sono affidati compiti e 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 informatica e 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 materiale non 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 documentazione eventualmente 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, è ammesso 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 lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di 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 di programmi, 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 posta elettronica anche all'Autorità Giudiziaria richiedente.

2.2.4 Accesso da remoto

Per motivi di assistenza, manutenzione, ricerca virus, attività di indagine sui malfunzionamenti, ricerca di anomalie o altre esigenze dell'organizzazione, la struttura competente in materia ICT può accedere da 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 connettività al 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, alle connessioni 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, solo laddove 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 rimarranno di proprietà dell'Amministrazione Regionale e l'assegnazione e disponibilità delle stesse sono "temporanee", nonché limitate all'esclusivo uso professionale. L'assegnazione delle risorse non implica un 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 necessità al 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 presente atto, 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 qualsiasi altro 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. In tali 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 devono ritenersi 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 provvedimenti disciplinari 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 competente in 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 server farm e delle postazioni

2.7.1 Tutela riservatezza, integrità, disponibilità e resilienza della rete 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 di difesa 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 parte dei 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, di misure di pseudonimizzazione, cifratura, minimizzazione ed in ogni altra tecnica di anonimizzazione dei 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 campione o 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 insieme di 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 inserimento della 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 comunicati dalla 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 sia più 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 password ai 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 cessazione avviene in automatico grazie alla sincronizzazione del database delle Risorse Umane con il servizio di autenticazione 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 di posta generiche, accesso a database e ad applicativi quali Paleo, Openact ecc.), in caso di cessazione del 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 riorganizzazione o 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 da parte 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 dei dati. 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 le relative periferiche (monitor, stampanti ecc.) devono essere spenti.

Oltre alle prescrizioni di cui al presente atto, tutti i Collaboratori sono tenuti anche all'osservanza delle regole 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 qualsiasi forma 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 possano compromettere 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'utilizzo della 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'ufficio o 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 (interne e/o esterne), stati di fatto, interazioni, attività o altro che possano comportare un rischio per la sicurezza e la riservatezza dei dati e delle informazioni.

3.8 Copia delle informazioni e gestione supporti strumenti portatili

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 in locale sui PC, anche in caso di formattazione semplice da parte di un esperto del settore), è consentita solo 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 essere custoditi 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 non controllata, 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 opportuna procedura 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 "Clean Desk" 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, supporti di 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 revisioni e 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 impatto sulla 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 "Clean Desk" 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 con una 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 abbiano particolare impatto sulla sicurezza e la riservatezza, il computer dovrà essere spento anche durante la giornata se 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 chiusi e 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 stessi devono 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 il loro uso, anche per assenze temporanee molto brevi.
14) Trattare i dispositivi di archiviazione di massa come CD-ROM, DVD, o unità USB / Pen Drive come 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, bacheche elettroniche, 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 su smartphone, 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 di accessi, 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 interna solo 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 delle stesse. 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 sostituto pro 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.