Deliberazione della Giunta Regionale 29 maggio 2023, n. 8-6951

Legge 7 agosto 2015 n. 124 e Legge 22 maggio 2017, n. 81. Approvazione Regolamento interno sull'utilizzo del lavoro agile per i dipendenti della Giunta Regionale ai sensi dell'art. 63, comma 2 del CCNL Funzioni Locali sottoscritto il 16 novembre 2022.

A relazione del Vicepresidente Carosso:

Premesso che

la Legge 7 agosto 2015 n. 124 "*Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche*" consente a ciascuna amministrazione, nell'ambito della propria autonomia organizzativa, di individuare modalità innovative, alternative al telelavoro, più adeguate rispetto alla propria organizzazione, ai fini della promozione nelle amministrazioni pubbliche della conciliazione dei tempi di vita e di lavoro e del miglioramento della qualità dei servizi erogati, fermo restando il rispetto delle norme e dei principi in tema di sicurezza sul luogo di lavoro, tutela della riservatezza dei dati e verifica dell'adempimento della prestazione lavorativa;

la legge 22 maggio 2017, n. 81, al capo II, disciplina quale modalità flessibile di esecuzione del rapporto di lavoro subordinato il "Lavoro Agile". Il lavoro agile è una modalità flessibile di esecuzione della prestazione lavorativa caratterizzata dallo svolgimento dell'attività lavorativa in parte all'interno dei locali aziendali e in parte all'esterno basata sulla flessibilità organizzativa e sulla volontarietà delle parti che sottoscrivono l'accordo individuale;

la direttiva n. 3/2017, recante le linee guida sul lavoro Agile nella Pubblica Amministrazione, del Dipartimento della Funzione Pubblica, ha fornito gli indirizzi per l'attuazione delle predette disposizioni attraverso una fase di sperimentazione. Tali linee guida contengono le indicazioni inerenti l'organizzazione del lavoro e la gestione del personale finalizzati, in particolare, alla promozione della conciliazione dei tempi di vita e lavoro dei dipendenti nell'ottica di favorirne anche il benessere organizzativo;

a seguito però dell'emergenza sanitaria determinata dalla pandemia da Covid-19, il lavoro agile è stato promosso nelle amministrazioni pubbliche quale "*modalità ordinaria di svolgimento della prestazione lavorativa*" per preservare la salute dei dipendenti pubblici. La Direttiva n. 1 del 25 febbraio 2020 del Dipartimento della Funzione Pubblica e i D.P.C.M. 8 marzo 2020 e 11 marzo 2020, hanno invitato le Amministrazioni, nell'esercizio dei poteri datoriali, a privilegiare e favorire modalità flessibili della prestazione lavorativa, individuando modalità semplificate e temporanee di accesso alla procedura, anche in deroga agli accordi individuali e agli obblighi informativi di cui agli articoli da 18 a 23 della legge 22.05.2017 n. 81;

a partire dal mese di marzo 2020, L'Amministrazione Regionale ha disciplinato, attraverso proprie circolari, le modalità straordinarie e temporanee di utilizzo del lavoro agile;

il successivo D.P.C.M. 23 settembre 2021 avente ad oggetto: "*Disposizioni in materia di modalità ordinaria per lo svolgimento del lavoro nelle pubbliche amministrazioni*" ha ritenuto che fosse oramai necessario superare la modalità di utilizzo del lavoro agile del periodo emergenziale, come una delle modalità ordinarie di svolgimento della prestazione lavorativa, per consentire alle pubbliche amministrazioni di dare il massimo supporto alla ripresa delle attività produttive e alle famiglie, attraverso il ritorno al lavoro in presenza come modalità ordinaria della prestazione lavorativa;

il D.M. del Ministro per la Pubblica Amministrazione in data 8 ottobre 2021, avente ad oggetto "*Modalità organizzative per il rientro in presenza dei lavoratori delle pubbliche amministrazioni"* e la Circolare del 5/01/2022 a firma dei Ministri della pubblica amministrazione e del lavoro e delle politiche sociali hanno attribuito ampia autonomia alle Pubbliche Amministrazioni nella individuazione delle modalità di attuazione del lavoro agile ("*ciascuna Amministrazione può equilibrare il rapporto di lavoro in presenza/lavoro agile secondo, le modalità organizzative più congeniali alla propria situazione*");

la D.G.R. n. 3-5226 del 21 giugno 2022 della Regione Piemonte ha approvato il Piano integrato di attività e organizzazione (PIAO) della Giunta regionale del Piemonte per gli anni 2022-2024, individuando un apposito punto 3.2. "*strategie e sviluppo di modelli innovativi di organizzazione del lavoro – lavoro Agile*" e prevedendo che "*L'amministrazione intende proseguire nel percorso di graduale introduzione del Lavoro Agile già previsti nel Piano della performance 2021-2023 delle strutture della Giunta regionale, attraverso l'adozione di una specifica disciplina finalizzata a tracciare il percorso amministrativo di accesso al lavoro Agile*";

da ultimo il CCNL Funzioni Locali sottoscritto il 16 novembre 2022 al Titolo VI, Capo I, ha disciplinato il lavoro agile stabilendo all'art. 63, comma 2, che "*il lavoro agile è una modalità di esecuzione del rapporto di lavoro subordinato, disciplinato da ciascun Ente con proprio Regolamento ed accordo tra le parti…*".

Ritenuto, alla luce della sopra elencata normativa, di procedere all'adozione del Regolamento interno (in seguito denominato "Regolamento") per l'applicazione del lavoro agile presso l'Ente; il Regolamento prevede che il lavoro agile - quale "*modalità flessibile di esecuzione della prestazione lavorativa per processi e attività di lavoro, connotata anche dallo svolgimento di parte dell'attività lavorativa all'esterno della sede di lavoro, anche senza precisi vincoli di orario o di luogo, entro i soli limiti di durata del tempo di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva e nel rispetto delle fasce di contattabilità*" - possa essere svolto dai dipendenti a tempo indeterminato e determinato, anche in regime di lavoro a tempo parziale, mentre è escluso per il personale dirigente, salvo che per eccezionali e temporanee esigenze, valutabili da parte del Direttore. Sono altresì esclusi i dipendenti che svolgono attività che, per le loro caratteristiche, non consentono di effettuare la prestazione lavorativa in modalità agile.

Dato atto che il Regolamento richiede che, nella scelta dei luoghi di svolgimento della prestazione lavorativa a distanza, debba essere garantita la presenza delle condizioni che assicurino la piena operatività della dotazione informatica e che debbano essere adottate tutte le precauzioni e le misure necessarie e idonee a garantire la più assoluta riservatezza sui dati e sulle informazioni che vengono trattate dal lavoratore stesso. A tal fine sono allegati al Regolamento (oltre al modello di richiesta di lavoro agile (allegato sub 1) e allo schema di accordo individuale(allegato sub 2) l'informativa sulla gestione della salute e sicurezza per i lavoratori ai sensi dell'art. 22 della legge n. 81/2017 (allegato sub 3) e il disciplinare della Regione Piemonte sull'uso degli strumenti informatici (allegato sub 4).

Dato atto che è stato esperito il confronto con le OOSS ai sensi dell'art. 5 del CCNL Funzioni Locali del 16.11.2022 e che il regolamento è stato trasmesso al CUG, presente anche alla riunione del 6.4.2023.

Vista la Legge 7 agosto 2015 n. 124;

vista la legge 22 maggio 2017, n. 81;

vista la direttiva n. 3/2017 del 1 giugno 2017 della Presidenza del Consiglio dei Ministri - Dipartimento della Funzione Pubblica, pubblicata il 14 giugno 2017;

visto il D.P.C.M. 23.09.2021;

visto il D.M. del Ministro per la Pubblica Amministrazione in data 08.10.2021;

visto il CCNL Funzioni Locali del 16.11.2021;

dato atto che la presente deliberazione non comporta oneri aggiuntivi a carico del bilancio regionale;

attestata la regolarità amministrativa del presente provvedimento ai sensi della D.G.R. n. 1-4046 del 17.10.2016 "Approvazione della "Disciplina del sistema dei controlli interni" parziale revoca della D.G.R. 8-29910 del 13.4.2000, come modificata dalla D.G.R. 1-3361del 14 giugno 2021.

Tutto quanto premesso e considerato, la Giunta regionale, a voti unanimi resi nelle forme di legge;

delibera

- di approvare, ai sensi dell'art. 63, comma 2 del CCNL Funzioni Locali sottoscritto il 16 novembre 2022, il Regolamento interno, e i relativi allegati (sub 1, 2, 3 e 4 descritti in premessa), sull'utilizzo del lavoro agile per i dipendenti della Giunta Regionale, allegati alla presente deliberazione per farne parte integrante e sostanziale, con decorrenza a far data dal 1 luglio 2023;

- di dare comunicazione della presente deliberazione a tutti i dipendenti della Giunta regionale attraverso la diffusione sulla intranet aziendale e con ogni altro mezzo idoneo;

- di dare atto che il presente provvedimento non comporta oneri per il bilancio regionale.

La presente deliberazione sarà pubblicata sul B.U. della Regione Piemonte ai sensi dell'art. 61 dello Statuto e dell'art. 5 della L.R. 22/2010 e in Amministrazione Trasparente ai sensi dell'art. 12 del D.Lgs. 33/2013.

(omissis)

Allegato

REGOLAMENTO INTERNO SULL'UTILIZZO DEL LAVORO AGILE
PER I DIPENDENTI DELLA GIUNTA REGIONALE

Art. 1
Definizione

1. Ai fini del presente Regolamento interno (di seguito denominato Regolamento) si intende per "Lavoro agile" una modalità flessibile di esecuzione della prestazione lavorativa per processi e attività di lavoro, connotata anche dallo svolgimento di parte dell'attività lavorativa all'esterno della sede di lavoro, anche senza precisi vincoli di orari o di luogo, entro i soli limiti di durata del tempo di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva, e nel rispetto delle fasce di contattabilità di cui all'art. 7, comma 7, del presente Regolamento.

Art. 2
Finalità e Principi generali

1. Il lavoro agile risponde alle seguenti finalità:
- introdurre nuove soluzioni organizzative che favoriscano lo sviluppo di un modello gestionale improntato alla flessibilità organizzativa per incrementare l'efficienza e l'efficacia dell'azione amministrativa;
- promuovere una visione dell'organizzazione del lavoro ispirata ai principi della flessibilità e dell'autonomia, responsabilizzando il personale e favorendo relazioni fondate sulla fiducia e sul lavoro di squadra;
- ottimizzare la diffusione di tecnologie e di competenze digitali, anche attraverso un'analisi dei processi ed una sempre maggiore digitalizzazione degli archivi e delle pratiche;
- facilitare le pari opportunità e le misure di conciliazione dei tempi di vita e di lavoro;
- promuovere la mobilità sostenibile tramite la riduzione degli spostamenti casa-lavoro-casa, nell'ottica di una politica ambientale sensibile alla diminuzione del traffico urbano in termini di volumi e di percorrenza.

2. Lo svolgimento della prestazione lavorativa in modalità agile viene regolamentata nel rispetto dei principi di cui alla Legge 81/2017, articoli da 18 a 23, e delle disposizioni del CCNL Funzioni Locali 2019-2021 del 16.11.2022; in particolare viene garantito il principio per il quale al lavoratore agile compete un trattamento economico e normativo non inferiore a quello complessivamente applicato nei confronti dei lavoratori che svolgono le medesime mansioni esclusivamente all'interno dell'amministrazione, nel rispetto dei contratti collettivi e integrativi vigenti.

3. E' garantito il diritto alla formazione, all'informazione, all'esercizio dei diritti sindacali e l'inclusione nei processi di misurazione e valutazione della performance, secondo il vigente sistema per la Performance dell'Ente e le disposizioni contrattuali collettive e integrative applicabili, e tenuto conto delle attività assegnate, nell'ambito della modalità agile di svolgimento della prestazione lavorativa, attraverso l'accordo individuale.

Art. 3
Destinatari

1. La prestazione lavorativa in modalità agile può essere resa da tutti i dipendenti a tempo indeterminato e determinato, anche in regime di tempo parziale.

2. La prestazione lavorativa in modalità agile è esclusa per il personale dirigente, salvo che per eccezionali e temporanee esigenze, valutabili da parte del Direttore, ed è esclusa per i dipendenti titolari di un contratto di lavoro da remoto.

3. La valutazione della richiesta di autorizzazione allo svolgimento della prestazione lavorativa in modalità agile, così come la definizione dei contenuti dell'accordo individuale con il dipendente, compete al Dirigente Responsabile del Settore cui il dipendente è assegnato. L'autorizzazione per i titolari di posizione organizzativa è di competenza del Dirigente Responsabile sentito il Direttore. Tutti gli accordi individuali sono sottoscritti dal Responsabile del Settore.

4. La modalità di lavoro agile è esclusa di norma nel periodo di prova previsto contrattualmente. Il Dirigente Responsabile della struttura di appartenenza può autorizzare lo svolgimento dell'attività in lavoro agile al dipendente in costanza del periodo di prova

previsto contrattualmente, previa valutazione della capacità di organizzazione autonoma dell'attività lavorativa assegnata.

5. La modalità di lavoro agile è esclusa nelle giornate in cui i dipendenti svolgono attività che richiedono necessariamente la presenza. In particolare:
- attività che prevedono ricevimento in presenza di pubblico;
- attività svolte dal personale addetto alla portineria, alla custodia e allo svolgimento di mansioni di autista;
- attività a tempo pieno di gestione degli archivi non dematerializzati.

6. La modalità di lavoro agile viene invece valutata caso per caso per:
- attività complesse di segreteria;
- attività che prevedono istruttorie tecniche multisettoriali e/o con soggetti esterni all'Amministrazione Regionale;
- attività che precludano la funzionalità della struttura di appartenenza e la qualità del servizio offerto;
- attività che per ragioni organizzative, anche temporanee, è necessario siano svolte in presenza.

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

1. Il Responsabile del Settore, prima di autorizzare lo svolgimento della prestazione lavorativa in modalità agile, deve valutare la sussistenza delle seguenti condizioni:
- la garanzia dell'invarianza dei servizi resi all'utenza;
- la mancanza di lavoro arretrato accumulato ancora da smaltire e, qualora ce ne fosse, la preventiva predisposizione di un idoneo e documentabile piano di smaltimento.

2. Il Responsabile del Settore deve garantire un'adeguata rotazione del personale autorizzato al lavoro agile, garantendo comunque il presidio dell'ufficio.

3. La domanda di autorizzazione al lavoro agile, redatta sull'apposito modulo allegato, deve essere indirizzata dal dipendente al Dirigente Responsabile della struttura di appartenenza e, per conoscenza, a lavoroagile@regione.piemonte.it.

4. La prestazione lavorativa svolta in modalità agile può essere resa per un numero massimo di giornate pari a 50 per unità di personale con rapporto di lavoro a tempo pieno e a tempo parziale orizzontale. Nel caso di rapporto di lavoro a tempo parziale verticale il numero di giornate da svolgere in modalità agile è riproporzionato, in relazione non solo al numero di giorni in cui è articolata la prestazione lavorativa, ma anche del monte ore settimanale. In caso di mobilità fra Direzioni o fra Settori, il numero di giornate in lavoro agile, riferite al dipendente interessato, può essere rimodulato in relazione a quanto previsto dall'art. 3, commi 5 e 6.

5. La prestazione lavorativa in modalità agile viene limitata ordinariamente a un giorno a settimana. Per specifiche esigenze (familiari o di organizzazione lavorativa) il numero massimo di giorni può essere elevato a 4 a settimana, sempre nel limite massimo di 50 giorni annuali.

6. L'Amministrazione si riserva di richiedere la presenza in sede del dipendente, in qualsiasi momento, per prevalenti esigenze di servizio, che di fatto impediscano di rendere la prestazione lavorativa in modalità agile, con un preavviso, di norma, di 24 ore e, comunque, con comunicazione che deve pervenire in tempo utile per la ripresa del servizio.

7. Il dipendente deve rendicontare i risultati conseguiti e le attività svolte, secondo modalità e criteri definiti dall'Ente e dal dirigente.

Art. 5
Accordo individuale

1. L'accordo individuale, redatto secondo apposito modello allegato al presente Regolamento, definisce i seguenti contenuti minimi, concordati dal Dirigente Responsabile del Settore di appartenenza e dal dipendente, sulla base delle esigenze organizzative, delle caratteristiche delle attività da svolgere e degli obiettivi:
- data di inizio e durata dell'accordo individuale;
- descrizione delle attività da svolgere in modalità agile;

- modalità di svolgimento della prestazione lavorativa in modalità agile anche con riferimento alle attività delle schede Piani di Lavoro del dipendente e agli ulteriori obiettivi specifici che possono essere assegnati nel corso dell'anno;
- indicazione del giorno in cui la prestazione viene di norma effettuata in modalità agile;
- indicazione dei luoghi (massimo 2) in cui verrà svolta l'attività, tali da garantire la protezione dei dati trattati, ai sensi dell'art. 10 del presente Regolamento;
- ipotesi di recesso, risoluzione e mancato rinnovo dell'accordo individuale;
- ipotesi di giustificato motivo del recesso;
- le fasce di contattabilità e i tempi di riposo del lavoratore;
- le modalità di esercizio del potere direttivo e di controllo del datore di lavoro;
- l'impegno del lavoratore a rispettare le prescrizioni indicate nell'informativa sulla salute e sicurezza sul lavoro agile ricevuta dall'amministrazione;
- riferimento al Regolamento sul lavoro agile nella Regione Piemonte e agli altri allegati all'accordo individuale, che il dipendente con la sottoscrizione dichiara di accettare e di rispettare.

2. Il testo dell'accordo individuale, con i relativi allegati, sottoscritto dal dipendente e dal Responsabile del Settore, viene trasmesso al Settore competente in materia di gestione giuridica del Personale per opportuna conoscenza e trattamento.

Art. 6
Luogo di lavoro

1. Fermo restando che la sede di lavoro resta invariata ad ogni effetto di legge e di contratto, il lavoro agile può essere svolto in luoghi diversi dalla propria abitazione purché i luoghi prescelti rispondano a requisiti di idoneità, nel rigoroso rispetto delle indicazioni fornite dall'Amministrazione in materia di protezione dei dati e di salute e sicurezza sul luogo di lavoro.

2. Nelle giornate di lavoro agile i/le dipendenti utilizzano spazi chiusi pubblici o privati; il dipendente avrà cura di svolgere la propria attività lavorativa in postazioni che garantiscano la necessaria riservatezza delle attività, evitando che soggetti esterni all'Amministrazione regionale possano facilmente venire a conoscenza di dati o notizie riservate.

3. E’ necessario fornire un’indicazione dei luoghi dove è resa la prestazione lavorativa, al fine della corretta copertura INAIL in caso di infortuni sul lavoro. Eventuali infortuni sul lavoro devono essere immediatamente comunicati alle strutture di appartenenza per le necessarie denunce.

4. luoghi di lavoro individuati dal lavoratore per lo svolgimento del lavoro agile devono essere collocati all’interno dei confini regionali, salvo specifiche e motivate esigenze, espressamente autorizzate dal responsabile. In ogni caso il lavoro agile non può essere svolto all’estero.

Art. 7
Rilevazione lavoro agile - Articolazione oraria

1. L’orario di svolgimento dell’attività in lavoro agile viene rilevato tramite l’utilizzo della procedura Iris web utilizzando l’apposita funzione (cd. “bollatrice virtuale”), nel rispetto dell’orario minimo previsto dalla tipologia oraria di ciascun dipendente e dalle fasce di contattabilità.

2. Per effetto della distribuzione flessibile del tempo di lavoro, nelle giornate di lavoro agile non sono riconosciute prestazioni di lavoro straordinario né eccedenza oraria o recupero di permessi, prestazioni di lavoro in turno notturno, festivo o feriale non lavorativo che determinino maggiorazioni retributive, missioni, lavoro disagiato, lavoro svolto in condizioni di rischio.

3. Per le giornate di attività in lavoro agile il dipendente non ha diritto all’erogazione del buono pasto, salvo obblighi derivanti dalla disciplina nazionale.

4. Nelle giornate di lavoro agile il dipendente, oltre ai giustificativi a giornata ed alle ferie ad ore, può fruire nelle fasce di contattabilità, ove ne ricorrano i relativi presupposti, dei permessi orari previsti dai contratti collettivi o dalle norme di legge.

5. Il dipendente che nelle giornate di lavoro agile, per sopraggiunti ed imprevisti motivi personali, si trovi nella condizione di impossibilità assoluta a rendere la prestazione di

lavoro deve darne tempestiva comunicazione al proprio dirigente e coprire l'assenza giornaliera con gli istituti previsti dal vigente CCNL.

6. Nel caso in cui il dipendente nelle giornate di lavoro agile non sia in grado di rendere la prestazione lavorativa per problemi di connessione o altri problemi legati al luogo di svolgimento del lavoro agile deve tempestivamente avvisare il proprio dirigente e rientrare in sede, completando la propria prestazione lavorativa fino al termine del proprio orario ordinario di lavoro.

7. Nelle giornate di lavoro agile per il dipendente valgono le seguenti regole:

a) fascia di contattabilità: dalle ore 10 alle ore 12.00 e dalle ore 14.00 alle 15.30. Il lavoratore in questa fascia deve rispondere sia telefonicamente che via mail o con altre modalità similari;

b) fascia di attività: all'interno della fascia 07.30 – 20.30, fatte salve le fasce di contattabilità di cui al punto a), il dipendente organizza autonomamente la propria prestazione lavorativa con riferimento al proprio debito orario giornaliero;

c) fascia di disconnessione: 20.30 – 7.30 (11 ore consecutive di riposo ai sensi dell'art. 7 del D.Lgs 66/2003); in tale fascia il lavoratore non può erogare alcuna prestazione lavorativa, né essere contattato telefonicamente, o via mail o con altre modalità similari.

8. Il comportamento del dipendente in servizio che, contattato non risponde per più volte e non provvede a richiamare, può essere valutato ai fini disciplinari.

9. Qualora il dipendente svolga l'attività in lavoro agile per più di sei ore consecutive deve, analogamente a quanto richiesto per lo svolgimento dell'attività in presenza, effettuare le pause previste dalla normativa vigente.

Art. 8
Dotazioni tecnologiche per lavoro agile

1. I dipendenti devono disporre di idonea dotazione tecnologica per lo svolgimento della prestazione lavorativa in forma agile, costituita da personal computer e strumenti per il collegamento da remoto ai servizi applicativi.

2. La connessione dati è sempre a carico del dipendente, fermo restando che questa deve garantire capacità di banda adeguata all'utilizzo del servizio RDS (indicativamente 5Mbps bidirezionale); è preferibile l'uso di connessioni di tipo dati (linea fissa xDSL/Fibra o Router Cellulare tipo "*saponetta*") e non ricorrere all'utilizzo della funzione di hot spot (o tethering) dello smartphone in quanto potenzialmente interrompibili dall'arrivo di chiamate vocali.

3. L'utilizzo di strumenti informatici personali è consentito nel rispetto delle disposizioni del disciplinare per l'uso degli strumenti informatici, che si applicano anche al lavoro agile. I dispositivi utilizzati devono essere dotati di sistema operativo supportato e regolarmente aggiornato. La connessione al sistema informativo dell'Ente con dispositivi personali è consentita solo attraverso la piattaforma RDS che garantisce l'indipendenza tra le risorse remote della rete regionale e quelle locali del dispositivo utilizzato.

4. In caso di necessità di supporto tecnico o in presenza di problematiche di sicurezza informatica che impediscano o ritardino sensibilmente lo svolgimento dell'attività lavorativa, anche in ordine a rischi di perdita o divulgazione di informazioni dell'Amministrazione, il dipendente è tenuto a darne immediata informazione al proprio responsabile e all'assistenza informatica, inviando una mail a hd_regione@csi.it. Qualora le suddette problematiche dovessero rendere impossibile la prestazione lavorativa, il dipendente può essere richiamato in sede.

Art 9
Monitoraggio

1. La prestazione di lavoro agile deve garantire il mantenimento di un livello quali-quantitativo e di risultati non inferiore a quello del lavoro in sede.

2. L'attività svolta in lavoro agile, analogamente a quanto previsto per l'attività lavorativa in sede, è oggetto di valutazione da parte del dirigente, in relazione a quanto rendicontato dal dipendente al dirigente, ai sensi dell'art. 4, comma 7.

3. In esito alla attività di monitoraggio definita ai punti precedenti, i dirigenti verificano l'attività prestata dal dipendente e il raggiungimento dei risultati attesi, anche confrontandosi con il dipendente stesso (per condividere punti di forza e di debolezza e risolvere eventuali problematiche).

Art. 10
Obblighi di custodia e riservatezza,

1. Nell'esecuzione della prestazione lavorativa in modalità agile, il dipendente è tenuto a garantire la riservatezza dei dati e delle informazioni trattate, persistendo il divieto di farne uso e/o comunicazione al di fuori delle finalità per le quali è autorizzato al trattamento dei dati.

2. Il dipendente è tenuto a partecipare alle specifiche iniziative di formazione organizzate dall'Amministrazione in materia di modalità operative del lavoro agile, aspetti di salute e sicurezza sui luoghi di lavoro e dei rischi connessi all'utilizzo dei dispositivi tecnologici, alle misure di sicurezza anche comportamentale sul corretto utilizzo e sulla tutela delle informazioni, dei beni o materiali della Regione Piemonte e alle previsioni normative in materia di privacy e tutela dei dati personali. In particolare, il dipendente è tenuto a segnalare tempestivamente ogni fatto che rilevi in tema di violazione della riservatezza dei dati trattati.

Art. 11
Sicurezza sul lavoro

1. La Regione Piemonte garantisce, ai sensi del decreto legislativo 9 aprile 2008, n. 81, la salute e la sicurezza del lavoratore in coerenza con l'esercizio dell'attività di lavoro in modalità agile e consegna al singolo dipendente un'informativa scritta con indicazione dei rischi generali e dei rischi specifici connessi alla particolare modalità di esecuzione della prestazione lavorativa. Il dipendente è tenuto a rispettare e ad applicare correttamente le direttive dell'Amministrazione e deve prendersi cura della propria salute e sicurezza, in linea con le disposizioni dell'art. 20 del D. Lgs. 81/08 comma 1.

2. La Regione Piemonte non risponde degli infortuni verificatisi a causa della mancata diligenza del lavoratore nella scelta di un luogo non compatibile con quanto indicato nell'Informativa.

Art. 12
Recesso e mancato rinnovo

1. Durante il periodo previsto per lo svolgimento del lavoro agile, ciascuna delle parti può, con adeguato preavviso, non inferiore a 30 giorni, recedere dall'accordo di lavoro agile, motivato se ad iniziativa dell'ente. Resta fermo quanto previsto dall'art. 19 – comma 2 – della Legge 81/2017 nel caso di lavoratori disabili ai sensi dell'articolo 1 della legge 12 marzo 1999, n. 68.

2. Costituisce giusta causa di recesso la modifica delle attività tale da rilevare ai sensi dell'art. 3 del presente Regolamento.

3. Nel caso in cui, in occasione del monitoraggio sulle attività svolte in lavoro agile, emergano due situazioni di significativa criticità in relazione agli aspetti qualitativi e quantitativi dell'attività svolta in modalità agile, il Responsabile del Settore lo comunica, per iscritto, al Direttore della Direzione, che congiuntamente al Responsabile stesso convocano il lavoratore; in relazione all'andamento del colloquio il dirigente responsabile, può disporre il rientro alle ordinarie modalità di prestazione lavorativa in presenza, a far data dal primo giorno lavorativo utile successivo alla comunicazione stessa.

4. In caso di orario debito/credito la reiterata carenza mensile oraria per flessibilità negativa (maggiore di meno 12 ore) riferita all'attività lavorativa resa in presenza, costituisce giustificato motivo di recesso dall'accordo individuale di lavoro agile.

5. Qualora, in corso di vigenza dell'accordo, il dipendente cambi struttura di assegnazione l'accordo in essere perde automaticamente efficacia e occorre procedere, ove il dipendente lo richieda, ad una nuova valutazione della sussistenza delle condizioni legittimanti l'applicazione del lavoro agile; lo stesso vale nel caso di modifica del contratto di lavoro (trasformazione da part time a full time e viceversa, da part time orizzontale a part time verticale).

Art. 13
Disposizioni finali

1. Il mancato rispetto di quanto previsto nel presente Regolamento costituisce violazione dei doveri di comportamento ed è valutabile ai fini disciplinari.

2. I 50 giorni annuali di lavoro agile possono essere aumentati nei seguenti casi:

a) in presenza di specifiche prescrizioni del medico competente;

b) in presenza di figli minori di 14 anni (in attesa di concessione del lavoro da remoto in caso di pratica già istruita con parere favorevole dal Settore competente in materia di gestione giuridica del personale);

c) su richiesta del Direttore e del Dirigente responsabile del dipendente, previa autorizzazione del Direttore della Giunta Regionale.

3. Per tutto quanto non previsto nel presente Regolamento trovano applicazione i contratti collettivi applicati alla Regione Piemonte, i regolamenti e le disposizioni interne di servizio e le norme di legge in materia di lavoro agile.

4. In relazione all'avvio delle attività nel Palazzo di V. Nizza n. 330 il Direttore della Giunta Regionale, sentita la Giunta Regionale, può adottare specifiche disposizioni derogatorie al presente regolamento.

5. Il presente Regolamento entra in vigore il 1° luglio 2023. Per l’anno 2023 Il numero dei giorni in cui la prestazione lavorativa può essere resa in modalità agile è riproporzionato in un massimo di 25 giorni per il personale a tempo pieno e in part-time orizzontale. Per il personale con contratto di lavoro a tempo parziale verticale il numero di giorni, sia per l’anno 2023 che annuali, è comunicato sulla Intranet dell’Ente.

Costituiscono allegati della presente disciplina i seguenti documenti:

1) Modello di richiesta di lavoro agile;
2) Schema di “Accordo individuale;

3) Informativa sulla gestione della salute e sicurezza per i lavoratori in Smart Working ai sensi dell’art. 22 L. n. 81/2017;

4) Disciplinare della Regione Piemonte sull’uso degli strumenti informatici.

Allegato 1

Al Direttore/Dirigente Responsabile
del Settore

e p.c. lavoroagile@regione.piemonte.it

Domanda di autorizzazione allo svolgimento della prestazione lavorativa in modalità agile

Il/la sottoscritto/a_____
in servizio presso_____
_____
con rapporto di lavoro
- full-time
- part time verticale: _____
- pert-time orizzontale: _____

CHIEDE

di poter accedere alla modalità di "lavoro agile" per lo svolgimento delle proprie attività

SI IMPEGNA

ad attenersi alle disposizioni impartite dall'Amministrazione per lo svolgimento del lavoro agile;

ad utilizzare le apparecchiature in conformità alle istruzioni e alle disposizioni ricevute;

a concordare preventivamente con il Dirigente Responsabile l'attività e la/le giornata/e della prestazione in modalità lavoro agile;

a svolgere l'attività in lavoro agile nel rispetto dei criteri di idoneità, sicurezza e riservatezza e in un luogo rispondente ai requisiti minimi stabiliti nella informativa sulla salute e sicurezza nel lavoro agile ai sensi dell'art. 22, comma 1, l. 81/2017;

ad adottare tutte le precauzioni necessarie a garantire la salvaguardia e lo svolgimento dell'attività in condizioni di sicurezza custodendo con massima cura tutte le informazioni;

a garantire la riservatezza dei dati e delle informazioni trattate, persistendo il divieto di farne uso e/o comunicazione al di fuori delle finalità per le quali è autorizzato al trattamento dei dati;

a svolgere la propria attività lavorativa in postazioni che garantiscano la necessaria riservatezza delle attività, evitando che soggetti esterni all'Amministrazione regionale possano facilmente venire a conoscenza di dati o notizie riservate.

Luogo e data, Firma del Dipendente

REGIONE PIEMONTE

allegato 2

ACCORDO INDIVIDUALE PER LA PRESTAZIONE DI LAVORO AGILE

Con il presente accordo individuale, tra la Regione Piemonte, in persona di (nome e cognome), Direttore/Dirigente del Settore _____ e la/il Signora/Signor_____nato/a_____ il_____a_____categoria_____in servizio presso la Direzione_____Settore_____ con tipologia di contratto (t. ind/ t. det -full time/ part time) _____

Vista la delibera di Giunta di approvazione del Regolamento Interno sull'utilizzo del lavoro agile per i dipendenti della Giunta regionale

si conviene quanto segue:

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

Art. 1
Avvio – durata – recesso

La/il Sig.ra/sig. _____a decorrere dal _____ e fino al _____ svolgerà la propria prestazione di lavoro anche in modalità agile.

Ognuna delle parti potrà recedere dal presente accordo con un adeguato preavviso, non inferiore a 30 giorni, motivato se ad iniziativa dell'ente.

Nel caso di lavoratori disabili il termine di preavviso del recesso da parte del datore di lavoro non può essere inferiore a novanta giorni.

In presenza di un giustificato motivo ognuna delle parti potrà recedere dal presente accordo senza preavviso a decorrere dal giorno successivo alla comunicazione alla controparte.

Qualora la/il sig.ra/sig._____ cambi struttura di assegnazione o nel caso di modifica del contratto di lavoro (trasformazione da part time a full time e viceversa, da part time orizzontale a part time verticale), l'accordo in essere perde automaticamente efficacia.

In caso do orario debito/credito la reiterata carenza mensile oraria per flessibilità negativa (maggiore di meno 12 ore) riferita all'attività lavorativa resa in presenza, costituisce giustificato motivo di recesso.

Costituisce giusta causa di recesso la modifica delle attività tali da non poter essere svolte in modalità agile.

Art. 2
Svolgimento del rapporto di lavoro

La prestazione lavorativa in lavoro agile è svolta per n. 1 giorno per settimana, presso _____(indirizzo prioritario), ed eventualmente presso _____(altro indirizzo).

Per specifiche esigenze (familiari o di organizzazione lavorativa) il numero massimo di giorni può essere elevato a 4 a settimana, sempre nel limite massimo di 50 giorni annuali; la richiesta e l'autorizzazione vengono comunicate tramite mail.

La programmazione delle giornate lavorative in modalità agile deve essere concordata preventivamente con il Dirigente, tenuto conto delle esigenze lavorative ed organizzative della struttura di appartenenza.

Il Dirigente può chiedere la presenza in sede della/del sig.ra/sig._____ in qualsiasi momento, per prevalenti esigenze di servizio, che di fatto impediscano di rendere la prestazione lavorativa in modalità agile, con un preavviso di norma di 24 ore e, comunque, con comunicazione che deve pervenire in tempo utile per la ripresa del servizio.

Art. 3

Attività lavorative, modalità di esecuzione e monitoraggio

La/il sig.ra/sig._____svolge in lavoro agile le seguenti attività, coerenti con il Piano di lavoro annuale:

1) _____

2) _____

3) _____

4) _____

Art. 4
Orario di lavoro

L'orario di svolgimento dell'attività in lavoro agile viene rilevato tramite l'utilizzo della procedura Iris web utilizzando l'apposita funzione - cd. "bollatrice virtuale" -, nel rispetto dell'orario minimo previsto dalla tipologia oraria di ciascun dipendente e dalle fasce di contattabilità.

Nelle giornate di lavoro agile valgono le seguenti regole:

a) fascia di contattabilità: dalle ore 10 alle ore 12.00 e dalle ore 14.00 alle 15.30. Il lavoratore in questa fascia deve rispondere sia telefonicamente che via mail o con altre modalità similari;

b) fascia di attività: all'interno della fascia 07.30 – 20.30, fatte salve le fasce di contattabilità di cui al punto a), il dipendente organizza autonomamente la propria prestazione lavorativa con riferimento al proprio debito orario giornaliero;

c) fascia di disconnessione: 20.30 – 7.30 (11 ore consecutive di riposo ai sensi dell'art. 7 del D.Lgs.n. 66/2003); in tale fascia il lavoratore non può erogare alcuna prestazione lavorativa, né essere contattato telefonicamente, o via mail o con altre modalità similari.

Qualora la/il sig.ra/sig_____ svolga l'attività in lavoro agile per più di sei ore consecutive deve effettuare le pause previste dalla normativa vigente.

Il dipendente che nelle giornate di lavoro agile, per sopraggiunti ed imprevisti motivi personali, si trovi nella condizione di impossibilità assoluta a rendere la prestazione di lavoro deve darne tempestiva comunicazione al proprio dirigente e coprire l'assenza giornaliera con gli istituti previsti dal vigente CCNL.

Art. 5
Strumenti di lavoro

Al fine di rendere possibile lo svolgimento della prestazione lavorativa il/la Sig. _____deve disporre di idonea dotazione tecnologica, costituita da personal computer e strumenti per il collegamento da remoto ai servizi applicativi.

La connessione dati è sempre a carico della/del sig.ra/sig_____, fermo restando che questa deve garantire capacità di banda adeguata all'utilizzo del servizio RDS (indicativamente 5Mbps bidirezionale); è preferibile l'uso di connessioni di tipo dati (linea fissa xDSL/Fibra o Router Cellulare tipo "*saponetta*") e non ricorrere all'utilizzo della funzione di hot spot (o tethering) dello smartphone in quanto potenzialmente interrompibili dall'arrivo di chiamate vocali.

L'utilizzo di strumenti informatici personali è consentito nel rispetto delle disposizioni del disciplinare per l'uso degli strumenti informatici, che si applicano anche al lavoro agile.

I dispositivi utilizzati devono essere dotati di sistema operativo supportato e regolarmente aggiornato.

La connessione al sistema informativo dell'Ente con dispositivi personali è consentita solo attraverso la piattaforma RDS che garantisce l'indipendenza tra le risorse remote della rete regionale e quelle locali del dispositivo utilizzato.

In caso di necessità di supporto tecnico o in presenza di problematiche di sicurezza informatica che impediscano o ritardino sensibilmente lo svolgimento dell'attività lavorativa, anche in ordine a rischi di perdita o divulgazione di informazioni dell'Amministrazione, il dipendente è tenuto a darne immediata informazione al proprio responsabile e all'assistenza informatica, inviando una mail a hd_regione@csi.it. Qualora le suddette problematiche dovessero rendere impossibile la prestazione lavorativa, il dipendente può essere richiamato in sede.

Il Dipendente ha l'obbligo di utilizzare e custodire gli strumenti di lavoro affidatigli con la massima cura e diligenza e nel rispetto delle norme in materia di salute e sicurezza sul lavoro.

Art. 6
Luogo di lavoro e sicurezza

La/il sig.ra/sig. _____ garantisce che i luoghi prescelti rispondano a requisiti di idoneità, nel rigoroso rispetto delle indicazioni fornite dall'Amministrazione in materia di protezione dei dati e di salute e sicurezza sul luogo di lavoro.

Il lavoratore si impegna:

- ad osservare le misure di prevenzione, protezione e comportamentali, impartite dal Datore di Lavoro nel documento "*Informativa sui rischi generali e si rischi specifici connessi alla particolare modalità di esecuzione del rapporto di lavoro*", ai sensi dell'art. 22, comma 1, Legge 81/2017;
- a prestare la dovuta attenzione per evitare che si producano situazioni pericolose o si verifichino infortuni;
- a non adottare condotte che possano generare rischi per la propria salute e sicurezza o per quella di terzi, sospendendo eventualmente la propria attività nel caso rilevi situazioni critiche.

Art. 7
Protezione e riservatezza dei dati

La/il sig.ra/sig _____ è tenuto a rispettare le normative comunitarie e nazionali sulla riservatezza e protezione dei dati in suo possesso e/o disponibili sul sistema informatico dell'Amministrazione, secondo le procedure stabilite dalla stessa, della cui corretta e scrupolosa applicazione il lavoratore è responsabile.

A tal fine il lavoratore è tenuto:

- ad adottare tutte le precauzioni necessarie a garantire la salvaguardia e lo svolgimento delle attività in condizioni di sicurezza custodendo con massima cura tutte le informazioni;

- a garantire la riservatezza dei dati e delle informazioni trattate, persistendo il divieto di farne uso e/o comunicazione al di fuori delle finalità per le quali è autorizzato al trattamento dei dati;
- a svolgere la propria attività lavorativa in postazioni che garantiscano la necessaria riservatezza delle attività, evitando che soggetti esterni all'Amministrazione regionale possano facilmente venire a conoscenza di dati o notizie riservate;
- a partecipare alle specifiche iniziative di formazione organizzate dall'Amministrazione in materia di modalità operative del lavoro agile, aspetti di salute e sicurezza sui luoghi di lavoro e dei rischi connessi all'utilizzo dei dispositivi tecnologici, alle misure di sicurezza anche comportamentale sul corretto utilizzo e sulla tutela delle informazioni, dei beni o materiali della Regione Piemonte e alle previsioni normative in materia di privacy e tutela dei dati personali. In particolare, il dipendente è tenuto a segnalare tempestivamente ogni fatto che rilevi in tema di violazione della riservatezza dei dati trattati.

Art. 8
Inadempimenti del lavoratore e sanzioni disciplinari

La prestazione lavorativa in modalità agile non modifica il potere direttivo del Dirigente di Responsabile, che viene esercitato con modalità analoghe a quelle applicate con riferimento alla prestazione resa presso i locali dell'Amministrazione
La/il sig.ra/sig_____ è tenuto al rispetto del Codice disciplinare e del Codice di comportamento dei Dipendenti del ruolo della Giunta Regionale.

Per quanto non espressamente previsto nel presente accordo si rinvia al Regolamento per la disciplina del lavoro agile adottato dalla Giunta Regionale.

Allegati:
- "Informativa sulla gestione della salute e sicurezza per i lavoratori in Smart Working ai sensi dell'art. 22 L. n. 81/2017";

- Disciplinare uso strumenti informatici allegato alla DGR 2-5456 del 3.8.2022.

Letto, confermato e sottoscritto

IL DIRIGENTE IL DIPENDENTE

_____ _____

VISTO

IL DIRETTORE per le PO_____

Allegato 3

REGIONE PIEMONTE

INFORMATIVA SALUTE E SICUREZZA

Informativa sulla gestione della salute e sicurezza per i lavoratori in Smart Working ai sensi dell'art. 22 L. n. 81/2017

PREMESSA

Il presente documento vuole dare un'informativa per coloro che svolgeranno la propria attività lavorativa in Smart Working (lavoro Agile).
L'informativa è predisposta e aggiornata a cadenza almeno annuale ai sensi dell'art. 22 della Legge n. 81/2017.
La presente informativa è consegnata in copia anche all'RLS (Rappresentante dei Lavoratori per la Sicurezza) come previsto dall'art. 22 della Legge, poiché questa figura ha un ruolo specifico nel sistema di prevenzione per l'attuazione degli adempimenti previsti in materia di salute e sicurezza di tutela e rappresentanza dei lavoratori.
Anche il lavoratore che opera in modalità di Smart Working si deve intendere come parte attiva della prevenzione e protezione della sua salute e sicurezza.
È compito dello Smart Worker mettere in atto ogni comportamento utile a limitare i rischi derivanti dell'esecuzione della prestazione lavorativa al di fuori dei locali dell'Amministrazione, 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 del lavoro.
Più in generale si può dire che lo Smart Worker:

- non potrà 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.

PRINCIPI GENERALI

I luoghi di lavoro individuati per l'esecuzione della prestazione lavorativa in Smart Working devono rispettare, per quanto possibile, le indicazioni previste per la sicurezza dei videoterminalisti.
Il lavoro dello Smart Worker non può prevedere un'esposizione a rischi diversi e ulteriori a quelli previsti durante la sua prestazione nel luogo di lavoro abituale presente nei locali dell'Amministrazione.
Nel seguito vengono riepilogate tali indicazioni.

IL 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 confort termico.

IL RISCHIO RUMORE

Le principali cause di rumorosità sono identificabili:

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

I lavoratori devono cercare un posto di lavoro il meno possibile rumoroso.

IL RISCHIO ELETTRICO

Durante l'esecuzione della prestazione lavorativa in Smart Working 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 e interruttori e attrezzature 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;
- verificare che l'attrezzatura utilizzata abbia la Marcatura CE;
- 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 presa;
- 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;
- non collegare tra loro spine incompatibili, utilizzando eventuali adattatori;

- l'utilizzo di prese multiple con numerose spine è assolutamente da evitare.

POSTAZIONE DI LAVORO

Il lavoro al videoterminale può causare l'insorgenza di disturbi muscolo scheletrici e affaticamento visivo.
Vediamo di seguito i principali criteri a cui il lavoratore deve fare riferimento per lavorare con il videoterminale in modalità di Smart Working:

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 da VDT

Il sedile di lavoro è fondamentale perché la postura assunta durante il lavoro sia corretta, in modo da minimizzare i possibili danni dovuti al fatto di mantenere per lunghi periodi una posizione seduta, deve fornire un supporto stabile ma deve anche permettere i cambiamenti di posizione (non devono esserci posizioni obbligate), inoltre deve avere caratteristiche che ne rendano confortevole l'uso.
Secondo le indicazioni del D.lgs. 81/08 il sedile deve essere di altezza regolabile, con gli spazi della seduta adattabile all'utilizzatore (quindi profondità della seduta e larghezza e altezza dei braccioli), avere un supporto lombare con altezza e inclinazione regolabili, avere superfici con bordi smussati, essere girevole per facilitare i cambi di posizione senza dover ruotare la colonna vertebrale, ed essere facile da spostare. Seduta e schienale devono essere in materiale traspirante, e tutto deve essere di facile pulizia.
Altre indicazioni relative al sedile riguardano la resistenza allo scivolamento della seduta (non deve essere possibile scivolarne fuori involontariamente), la presenza di una base a 5 razze

antiribaltamento e di rotelle per facilitare gli spostamenti (sia per entrare e uscire dalla postazione, sia per spostarsi ad esempio per prendere un oggetto). La sedia non deve potersi spostare accidentalmente, o quando non è occupata: le caratteristiche di attrito delle rotelle vanno valutate a seconda delle caratteristiche del pavimento.
Per alcune condizioni di lavoro in cui si usa la posizione reclinata (ad esempio controllo di schermi posti più in alto della testa) lo schienale deve fornire un supporto sicuro anche per le scapole.
I braccioli devono essere regolabili e, soprattutto, non devono essere un ostacolo alla vicinanza con il piano di lavoro (devono permettere che la sedia entri sotto il piano di lavoro).

CRITERI PER LA PREVENZIONE DI DISTURBI VISIVI

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

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

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

Le misure di prevenzione da porre in essere sono di carattere ambientale e comportamentale:

- Il monitor dev'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 e inclinabile;
- 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.

CRITERI PER LA PREVENZIONE DI DISTURBI OSTEOMUSCOLARI

La maggior parte dei problemi creati dall'uso di VDT dipende dalla postura assunta dal lavoratore. Basta un'errata postura (anche senza sforzi particolari) perché il lavoratore subisca ripercussioni a livello di schiena.
Postazioni di lavoro inadeguate dal punto di vista della disposizione degli arredi e del terminale, il mantenimento per periodi prolungati di posizioni di lavoro fisse 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 rischio 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 illuminazione troppo forte e privi di schermatura alle finestre;
- 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 lo Smart Worker sia oggetto d'infortunio deve fornire dettagliata e tempestiva informazione sull'evento all'Amministrazione secondo le modalità individuate nel contratto.

allegato 4

REGIONE PIEMONTE

DISCIPLINARE PER L'UTILIZZO DEI SISTEMI INFORMATICI

Sommario

Premessa

Il presente disciplinare intende fornire le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.

Ogni utente, intendendosi con ciò ogni dipendente, senza distinzione di ruolo e/o di livello e ogni collaboratore ed organo politico in possesso di specifiche credenziali di autenticazione per l'accesso alle risorse informatiche dell'Ente, è tenuto a rispettare il presente disciplinare, che è reso disponibile tramite le modalità specificate al punto 20.

Si specifica che tutti gli strumenti utilizzati dagli utenti per prestare la propria attività lavorativa, intendendo con ciò, ad esempio, PC, notebook, strumenti informatici, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "strumenti"), sono messi a disposizione dall'Ente, come dispositivi o come servizio (DaaS – Desktop as a service); ma è anche consentito l'utilizzo di dispositivi propri (BYOD[1]) per rendere la prestazione lavorativa al di fuori della rete regionale.

In ogni caso, sui dispositivi di proprietà degli utenti, sia utilizzati come terminali del desktop remoto, sia per accedere a risorse disponibili sul web, non sono previste né l'installazione di programmi e/o procedure regionali né l'impiego di alcun sistema di monitoraggio delle attività e/o delle connessioni.

Le disposizioni contenute nel presente disciplinare si applicano, a compendio delle regole definite dall'Ufficio competente, anche ai dispositivi mobili (smartphone e tablet) in grado di interconnettersi all'infrastruttura di rete ed ai relativi servizi.

I dati personali e le altre informazioni degli utenti, registrati automaticamente negli strumenti durante il loro uso (log di sistema), sono memorizzati sugli strumenti stessi e possono essere utilizzati per la sicurezza del lavoro e per la tutela del patrimonio; per "tutela del patrimonio" si intende altresì la sicurezza informatica e la tutela del sistema informatico.

Tali informazioni sono raggiungibili solo dall'amministratore di sistema, nei casi previsti dalla Legge, con gli strumenti nativi dei sistemi operativi.

Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

1 Oggetto e finalità

1.1 Il presente Disciplinare è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;

1 Bring Your Own Device

- in attuazione del Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR);

1.2 La finalità del presente disciplinare è quella di promuovere in tutti gli utenti una corretta "cultura informatica", definire le norme di comportamento per l'uso degli strumenti messi a disposizione dall'amministrazione, fornire le indicazioni necessarie per evitare il verificarsi di qualsiasi uso non conforme o abuso dei succitati strumenti ed informare gli utenti rispetto alle attività memorizzate nei log di sistema.

2 Principi generali e principi di riservatezza nelle comunicazioni

2.1 I principi che sono a fondamento del presente Disciplinare sono gli stessi espressi nel GDPR, e, precisamente:

a il principio di liceità, secondo il quale ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 del GDPR: consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

b il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/16);

c il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori;

d i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 5, commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

2.2 L'utente si attiene alle seguenti regole di trattamento dati:

a è vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, particolari e giudiziari, elementi e informazioni dei quali l'utente viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al Responsabile della struttura in cui opera;

b è vietata l'estrazione per uso personale di originali e/o copie cartacee ed informatiche di documenti, fascicoli, lettere, data base e quant'altro.

2.3 Le misure per il trattamento dei dati personali e le procedure da adottarsi in caso di *data breach* sono contenuti in appositi provvedimenti adottati dalla Giunta Regionale[2].

2 Il link contenuto nel testo è operativo solo se la consultazione avviene all'interno della rete regionale

2.4 L'Amministrazione regionale effettuerà, inoltre, attività di monitoraggio e verifica dell'efficacia delle misure di protezione predisposte sul sistema informativo rispetto ad aggressioni esterne senza che siano necessarie preventive ulteriori informative. Le risultanze di tali attività di monitoraggio e verifica potranno essere utilizzate soltanto in modo proporzionato e pertinente alle finalità e alla natura delle stesse e non, ad esempio, al fine di attuare indirettamente un controllo a distanza dell'attività lavorativa svolta dall'utente.

3 Tutela del lavoratore

3.1 Alla luce dell'art. 4, comma 1, L. n. 300/1970, le disposizioni di cui al presente disciplinare non sono finalizzate all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze di servizio e di sicurezza nel trattamento dei dati personali.

3.2 È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 679/16.

4 Descrizione dell'architettura dei servizi informatici

4.1 Ogni postazione di lavoro all'interno degli uffici regionali è dotata di una connessione di rete aziendale sulla quale transitano sia i servizi informatici che quelli di telefonia fissa (VoIP).

4.2 In aggiunta alla connessione di rete tramite cavo, può essere disponibile il servizio di rete Wi-Fi; attraverso la tecnologia Wi-Fi è possibile connettersi sia alla rete aziendale identificata dal SSID "GR-WiFi", che prevede l'autenticazione automatica dei dispositivi dell'Ente iscritti al dominio mediante protocollo 802.1x, sia alla rete pubblica denominata "Wi-Pie la rete per tutti", la cui fruizione è disciplinata da apposito Regolamento regionale.

4.3 Attraverso qualsiasi dispositivo idoneo collegato alla rete (sia aziendale che internet) ogni utente può connettersi al proprio desktop remoto personale (RDS). Negli uffici regionali è previsto anche l'utilizzo di dispositivi con sistema operativo locale per la fruizione di programmi non disponibili in ambiente RDS.

4.4 Ai sensi dell'art. 6, comma 2, della L.R. 26 marzo 2009, n. 9, la Giunta regionale nella scelta dei programmi per elaboratore elettronico, privilegia quelli appartenenti alla categoria del software libero e i programmi il cui codice è ispezionabile dal titolare della licenza. Qualora si renda necessaria l'acquisizione di programmi software, si adottano le prescrizioni di cui al Codice dell'Amministrazione Digitale (CAD) e alle relative Linee guida definite dall'Agenzia per l'Italia Digitale (AgID).

5 Il referente SiRe

5.1 Ogni Assessorato ed ogni Direzione regionale nomina:

- almeno un dipendente, tra il personale assegnato, nel ruolo di referente SiRE Asset, con funzioni di supporto a tutti i processi relativi alle postazioni di lavoro dell'Ente e ai servizi informatici;

- almeno un dipendente, tra il personale assegnato, nel ruolo di referente SiRE ICT, con funzioni di supporto allo sviluppo del Sistema Informativo nell'ambito della propria Direzione;

I ruoli di referente SIRe Asset ed ICT possono essere svolti, nell'ambito della Direzione/Assessorato, dalle medesime persone.

6 Gestione, assegnazione e revoca delle credenziali di accesso al dominio, alla posta elettronica, alle procedure con autenticazione Apriride e alle procedure con autenticazione propria.

6.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate secondo le indicazioni fornite dal tavolo di coordinamento tra i Settori regionali competenti a definire il processo di de/provisioning e moving del personale.

6.2 Le credenziali di autenticazione relative ai diversi ambiti, consistono in:

- una username per l'accesso al dominio *regpient01* e relativa password;
  - per i dipendenti dell'Ente la username coincide con la matricola;
  - per le altre persone abilitate ad accedere al dominio (collaboratori/organi politici) la username è personalizzata in funzione della tipologia contrattuale in essere con l'Amministrazione (UNR, RAS, ……)
- una login per l'accesso al sistema di posta elettronica e servizi di rete (psnet) associati, del tipo nome.cognome@regione.piemonte.it ovvero per i collaboratori del tipo nome.cognome@mail.regione.piemonte.it e relativa password; è garantita la gestione di credenziali univoche in caso di omonimia;
- un certificato digitale per l'accesso alle procedure che ne richiedono l'uso con relativo codice di installazione, richiesto ad ogni accesso al dominio, fornito dal CSI Piemonte;
- altre credenziali, per servizi esterni ad Apriride, con autenticazione propria.

6.3 Per ogni evento riguardante ciascun utente (assunzione, cessazione, mobilità) la procedura di Alerting provvede alla tempestiva informazione della variazione agli uffici deputati alla gestione delle credenziali medesime.

6.4 Abilitazioni, disabilitazioni e profilazione nell'accesso alle procedure e/o alle cartelle di rete avvengono, su istanza del Dirigente/Direttore e ad opera del referente SIRe Asset, in coerenza alle modalità di svolgimento delle funzioni e delle singole attività all'interno dell'Ente e nel rispetto della normativa in materia di privacy. È cioè necessario che ogni Dirigente e Direttore consideri come le singole attività sono attribuite e svolte dai dipendenti loro assegnati con particolare attenzione alla configurazione del trattamento dei dati personali che ne deriva e alle relative autorizzazioni e profilazioni specifiche per utente e per applicativo utilizzato. Analoga procedura si applica per gli Assessorati in funzione dell'organizzazione dei relativi uffici di comunicazione.

6.5 Le credenziali di accesso alle risorse informatiche devono essere periodicamente modificate e rispettare regole di sicurezza nella loro composizione. Il periodo di validità e le regole applicate possono variare a seconda degli applicativi interessati (di norma la password deve rispettare 3 dei seguenti requisiti minimi di complessità: almeno 8 caratteri, uso di lettere maiuscole e minuscole, numeri e caratteri speciali oltre, preferibilmente a non contenere parole di senso compiuto).

6.6 In caso l'utente dimentichi (o faccia scadere) la password di accesso ad un servizio, se non è disponibile una procedura autonoma, presenterà richiesta di reset della stessa all'ufficio competente che verificherà l'identità del richiedente prima del rilascio della nuova password.

7 Strumenti informatici (PC - fisico o desktop remoto, notebook e altri strumenti con relativi software e applicativi) di proprietà dell'Ente.

7.1 L'utente è consapevole che gli strumenti di proprietà dell'Ente sono forniti per rendere la prestazione lavorativa e per scopi professionali, estendendo a tale ambito anche quelli connessi alla ricerca, alla didattica e alla crescita delle competenze nell'uso delle tecnologie dell'informazione e della comunicazione. Ognuno è responsabile dell'utilizzo degli strumenti assegnati dall'Amministrazione ed ha il compito di farne un uso conforme ai principi di diligenza sanciti dal codice civile; ciascun utente si deve quindi attenere alle regole di utilizzo degli strumenti di cui al presente disciplinare.

7.2 L'accesso agli strumenti è protetto da password; per il primo accesso devono essere utilizzate le credenziali fornite dall'Amministratore di sistema (cfr. punto 6.2), la password deve essere quindi modificata dall'utente con una personale. A tal proposito si rammenta che le credenziali sono strettamente private e l'utente è tenuto a conservarle nella massima segretezza.

7.3 Ogni dispositivo hardware assegnato, identificato univocamente da un numero di censimento informatico, deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione delle password d'accensione (BIOS) e protezione disco, senza preventiva autorizzazione da parte dell'Amministratore di sistema.

Ogni dispositivo hardware, indipendentemente dall'assegnazione, può essere utilizzato da tutti gli utenti in possesso delle credenziali di accesso al dominio; nel caso di dispositivi con sistema operativo Windows viene creata un'area riservata sul disco locale per ogni utente che ha avuto accesso allo stesso, nel caso di dispositivi configurati per l'accesso diretto ad RDS non viene memorizzato alcun dato in locale.

Al fine di garantire la riservatezza e sicurezza dei propri dati è necessario memorizzarli sulle share di rete (cfr. punto 8 – infrastruttura di rete).

7.4 Le impostazioni dei personal computer e dei relativi programmi per elaboratore installati sono predisposte dagli addetti informatici incaricati secondo standard decisi dall'Amministrazione regionale e volti a garantire la fruizione di tutti i servizi necessari allo svolgimento delle mansioni degli utenti.

L'utente non può modificarle autonomamente; può ottenere cambiamenti nelle impostazioni solo previa autorizzazione da parte del Settore competente, su richiesta del referente SIRe Asset

attraverso la procedura definita, in funzione di particolari attività che necessitano di software o impostazioni *ad hoc*.

7.5 L'installazione sui personal computer di sistemi operativi e programmi applicativi e, in generale, di software, avviene generalmente ad opera dei tecnici informatici incaricati, che operano seguendo i necessari criteri di sicurezza. L'uso di tali programmi deve avvenire nel rispetto dei contratti di licenza che li disciplinano e delle specifiche prescrizioni di volta in volta indicate.

7.6 L'installazione di programmi da parte dell'utente, ove sia consentito dal personal computer e dalle relative impostazioni, deve avvenire senza aggirare divieti o restrizioni eventualmente previsti, nel pieno rispetto delle condizioni che disciplinano l'utilizzo di tali programmi e, in generale, della normativa vigente, con particolare riferimento alle disposizioni in materia di protezione di diritti di proprietà intellettuale: abusi o utilizzi illeciti saranno puniti conformemente alle disposizioni che disciplinano il rapporto di lavoro. In ogni caso, l'utente sarà responsabile e sarà chiamato a manlevare e tenere indenne l'Amministrazione regionale da qualsiasi danno o richiesta di risarcimento che venga avanzata da soggetti terzi.

7.7 Tutti i software presenti sui Personal Computer al momento della consegna ed in particolare i software necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi dagli utenti.

7.8 L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la postazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare uno strumento incustodito con una sessione di lavoro attiva può essere causa del suo utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

7.9 È obbligatorio consentire l'installazione degli aggiornamenti di sistema operativo che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.

Per gli aggiornamenti degli applicativi proposti durante il loro uso è necessario l'intervento dell'Amministratore di Sistema che provvederà a rilasciarli dopo averne verificato la compatibilità con le policy di sicurezza e con i sistemi informativi coinvolti.

7.10 È vietato utilizzare i dispositivi informatici per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

7.11 È vietato connettere alla rete locale cablata o alla rete Wi-Fi dipendenti (GR-WiFi) qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di sistema.

7.12 Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, è tenuto a comunicarlo tempestivamente all'Help Desk (cfr. punto 9).

7.13 In regime di telelavoro e lavoro agile si applicano anche le ulteriori disposizioni previste dai relativi disciplinari e dai contratti individuali.

7.14 In caso di furto e/o smarrimento è compito dell'utente assegnatario dell'attrezzatura presentare denuncia all'autorità giudiziaria ed informare, inoltrando copia della denuncia presentata, il proprio referente SIRe Asset e i Settori coinvolti nella gestione delle attrezzature.

8 Infrastruttura di rete e File System

8.1 Il dominio dell'Ente, *regpient01*, comprende tutti i servizi di identificazione utente e accesso personalizzato alla rete aziendale, al suo file system e alle altre risorse di rete e di stampa condivise.

8.2 Per l'accesso al dominio dell'Ente, ciascun utente deve essere in possesso di credenziali di autenticazione secondo quanto previsto al punto 6.2

8.3 È vietato accedere alla rete ed ai sistemi informativi utilizzando credenziali di altri utenti.

8.4 L'accesso al dominio garantisce all'utente la disponibilità dei dispositivi multifunzione di stampa e delle seguenti share di rete (cartelle condivise su server):

- home directory, identificata con la lettera H:/, denominata come la username ed accedibile esclusivamente dall'utente[3];
- cartella condivisa della struttura di assegnazione;
- cartella comune denominata *common*, utilizzabile da tutti gli utenti del dominio, destinata allo scambio di documenti e file, nel rispetto della normativa privacy[4], tra utenti di strutture diverse; i contenuti di questa cartella vengono automaticamente cancellati tutte le notti;
- eventuali altre cartelle condivise, rese disponibili secondo specifica abilitazione (cfr. 6.4).

Tutte le cartelle di rete, siano esse condivise o personali, ospitano esclusivamente contenuti professionali e sono quotidianamente oggetto di backup.

8.5 Tutte le risorse di memorizzazione, diverse da quelle citate al precedente punto 8.4 non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o in disponibilità personale come hard disk portatili o NAS[5] ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse, poiché la sicurezza e la protezione contro la loro eventuale perdita non sono garantite; pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

8.6 Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, dell'utente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività delle strutture sia necessario accedere a documenti di lavoro presenti sui dispositivi o sulla share personali, l'utente può delegare, in accordo con il proprio Responsabile, a un altro dipendente della sua stessa struttura a sua scelta ("fiduciario") il compito di individuare e inoltrare al Responsabile della struttura a cui è assegnato i documenti rilevanti per lo svolgimento dell'attività lavorativa.

3 Le cartelle personali sono di dimensione limitata e uguale per tutti gli utenti, in quanto documenti e file di lavoro devono essere di norma memorizzati nelle cartelle condivise della propria struttura o gruppo di lavoro.

4 Qualora siano coinvolti dati personali, l'utente dovrà adottare tutte le precauzioni e le misure per garantire la sicurezza e l'immodificabilità del o dei file originali (salvataggio crittografato con password e impronta SHA-256)

5 Network Attached Storage

La delega si esprime come richiesta all'amministratore di sistema, da effettuarsi tramite il referente SIRe Asset, di temporanea abilitazione al fiduciario ad accedere ai dispositivi o alla share personale dell'utente.

Delle attività svolte dal referente SIRe e dal fiduciario deve essere informato l'utente interessato.

8.7 Qualora l'utente non abbia delegato un suo fiduciario, secondo quanto sopra specificato, in caso di straordinaria necessità ed urgenza, il Responsabile della struttura a cui è assegnato l'utente può richiedere, tramite il referente SIRe Asset, con apposita e motivata richiesta all'Amministratore del Sistema, di accedere alla share e/o ai dispositivi dell'utente assente, in modo di prendere visione delle informazioni e dei documenti necessari; di tale attività deve essere redatto apposito verbale e informato l'utente interessato.

8.8 E' consentito trasferire documenti elettronici dai sistemi informativi e strumenti dell'ente a/da dispositivi esterni (hard disk, chiavette usb, cd, dvd e altri supporti) nei casi previsti (DGR 1-7108 del 29 giugno 2018 recante: "Disposizioni in materia di accesso civico e di accesso civico generalizzato per le strutture della Giunta regionale del Piemonte" e DGR 8-854 del 23 dicembre 2019 "Disciplina per gli uffici della Giunta regionale relativa alle modalità di rilascio di documenti amministrativi e tariffario per il rimborso dei costi sostenuti dall'amministrazione regionale. Revoca DGR n. 39-4814 del 17.12.2001") e per temporanee esigenze di lavoro, al termine delle quali le copie devono essere cancellate.

8.9 Nei rapporti con soggetti esterni all'Amministrazione è consentito l'utilizzo di strumenti di condivisione file di grandi dimensioni sul cloud, fatto salvo il rispetto delle prescrizioni di cui al Regolamento Europeo 679/16 "General Data Protection Regulation", quando le caratteristiche dei file non ne consentono la gestione con gli ordinari strumenti a disposizione degli utenti. In questo caso, l'utente dovrà adottare tutte le precauzioni e le misure per garantire la sicurezza e l'immodificabilità del o dei file originali oggetto del trasferimento (salvataggio crittografato con password e impronta SHA-256). Gli strumenti utilizzabili sono quelli già preventivamente verificati e resi disponibili dall'Amministratore di sistema.

8.10 Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia delle cartelle su server, con cancellazione dei file obsoleti o inutili: particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

8.11 L'Amministratore di sistema si riserva la facoltà di negare o interrompere l'accesso alla rete ai dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica.

8.12 Per gli utenti che erogano la propria prestazione lavorativa in modalità di telelavoro o lavoro agile si applicano anche le disposizioni di cui ai relativi disciplinari.

9 Help Desk[6]

9.1 In caso di malfunzionamento di strumenti e/o servizi del sistema informativo regionale l'utente deve segnalarlo, in prima persona o tramite il referente SIRe Asset, al servizio di Help Desk.

9.2 Il servizio di Help Desk è raggiungibile mediante il numero telefonico interno 82888 (800282888 da rete pubblica) o mediante l'indirizzo mail hd_regione@csi.it.

9.3 A fronte della segnalazione telefonica il servizio di Help Desk cerca di formulare una diagnosi del malfunzionamento intervenendo direttamente per quanto possibile o inoltrando la richiesta di assistenza al supporto di secondo livello interessato.

9.4 Per ogni segnalazione registrata, il servizio di Help Desk è tenuto ad aprire un ticket di assistenza e darne visibilità all'utente. Lo stesso ticket verrà chiuso a fronte della risoluzione del problema e anche della chiusura deve essere informato l'utente originatore della segnalazione.

10 Regole applicabili all'utilizzo di internet mediante gli strumenti informatici dell'Ente[7]

10.1 La rete internet può e deve essere utilizzata dall'utente a supporto dell'attività lavorativa.

10.2 L'accesso ad internet dalla rete privata regionale avviene attraverso un servizio "proxy" ed è filtrato da un ulteriore servizio di sicurezza che inibisce l'accesso a siti potenzialmente malevoli e/o manifestamente inopportuni sulla base di una "black list" costantemente aggiornata. È possibile richiedere, attraverso il referente SIRe Asset lo sblocco dalla black list di siti erroneamente inseriti nella stessa.

10.3 È favorito l'uso, di norma attraverso l'interfaccia web, di strumenti di messaggistica istantanea e servizi di videoconferenza e collaborazione on line, per permettere una efficace e comoda comunicazione sia tra i colleghi, sia con interlocutori esterni all'Ente. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche e alle e-mail.

11 Utilizzo della posta elettronica istituzionale

11.1 Ad ogni utente viene fornito un account e-mail nominativo.

11.2 L'insieme degli indirizzi di posta nominativi costituisce la rubrica globale della Regione Piemonte ed è disponibile nella piattaforma di gestione della posta. Trattandosi di dati personali possono essere divulgati esclusivamente per fini istituzionali.

11.3 L'Ente fornisce, altresì, delle caselle di posta elettronica condivise associate a unità organizzative, uffici o gruppi di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative per le comunicazioni di tipo procedimentale. È compito del referente SIRe Asset richiedere la

6 I dettagli relativi al funzionamento del servizio di Help Desk sono disponibili alla relativa pagina pubblicata sulla Intranet regionale (link operativo solo per consultazione all'interno della rete regionale)

7 Le regole specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007 e s.m.i..

creazione e/o la eliminazione delle caselle di posta condivise e gestire le abilitazioni e/o disabilitazioni degli utenti alle stesse, definendone il relativo livello di delega.

11.4 L'utilizzo dell'e-mail deve essere finalizzato allo svolgimento delle proprie mansioni lavorative e alle comunicazioni relative alle stesse, conformemente al punto 7.1. Si ricorda che gli indirizzi delle caselle di posta elettronica forniti dall'Ente di norma non devono essere utilizzati, in particolare in modo massivo, per fini non connessi all'attività lavorativa. (ad esempio l'invito a partecipare ad eventi extra lavorativi).

11.5 È compito di ogni utente provvedere alla costante eliminazione delle mail non necessarie al fine di contenere le dimensioni degli archivi di posta. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle cartelle di rete.

11.6 L'iscrizione a mailing-list o newsletter esterne con l'indirizzo fornito dall'Amministrazione è ammessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

11.7 Allo scopo di garantire sicurezza alla rete, l'utente deve evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito oppure che contengono allegati con contenuto di tipo attivo come, ad esempio, *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza è opportuno contattare il referente SIRe Asset o l'Help Desk per una valutazione dei singoli casi.

11.8 Non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

11.9 Nel caso fosse necessario inviare allegati "pesanti" (oltre ai 10 MB) è opportuno ricorrere alla compressione dei file originali in un archivio di formato .zip o equivalente e agli strumenti di pubblicazione di file disponibili nel sistema di posta. Per esigenze particolari, è consentito il ricorso agli strumenti cloud raggiungibili dalla rete dell'Ente, coerentemente a quanto disposto al punto 8.9.

11.10 Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso criptazione con apposito software (archiviazione e compressione con password). La password di criptazione deve essere comunicata al destinatario possibilmente attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e comunque mai insieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza possono essere inviati soltanto a destinatari – persone o Enti – qualificati e competenti.

11.11 Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un avviso di assenza facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza oppure indicando un indirizzo email alternativo preferibilmente di tipo condiviso, del

tipo settore@regione.piemonte.it. Si rammenta che ciascun utente ha il diritto alla disconnessione e il diritto di non dover presidiare la propria casella di posta elettronica nel periodo di ferie, poiché le stesse sono destinate al recupero psico-fisico delle energie (cfr. L. 81/2017).

11.12 Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, dell'utente, qualora per necessità delle strutture sia necessario accedere alla sua casella di posta, il titolare della casella di posta ha la facoltà di delegare un altro utente, denominato "fiduciario", per verificare il contenuto di messaggi e per inoltrare al Responsabile della propria struttura quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. La delega si esprime attraverso l'apposita funzione presente sull'interfaccia della mail istituzionale.

11.13 Nel caso non sia presente nemmeno il fiduciario, solo in casi di straordinaria necessità ed urgenza e per ragioni di sicurezza, il Responsabile della struttura a cui è assegnato l'utente assente potrà richiedere all'Amministratore di sistema di accedere alla sua casella di posta. Sarà compito del Responsabile della struttura assicurarsi che sia redatto un verbale attestante quanto avvenuto e che venga informato il lavoratore interessato.

11.14 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti al servizio, possibilmente su autorizzazione del Responsabile della struttura competente. Per evitare violazioni della privacy per diffusione degli indirizzi di posta nonché che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo e indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.

11.15 È consentito inviare messaggi di posta elettronica in nome e per conto di un altro utente solo su sua espressa autorizzazione formale o delega.

11.16 I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi contenenti virus riconosciuti vengono eliminati dal sistema.

11.17 Nel caso in cui l'utente non presti più la sua attività lavorativa presso la Giunta Regionale del Piemonte, la casella di posta elettronica nominativa sarà disattivata appena l'ufficio incaricato della gestione delle credenziali di posta riceve l'informazione dalla procedura di Alerting (cfr. punto 6.3); contestualmente si provvederà alla cancellazione del contenuto "on line".

11.18 Prima della cessazione dal servizio, l'utente è tenuto ad impostare una risposta automatica che informa di tale cessazione e indica un indirizzo mail alternativo, preferibilmente di gruppo, cui rivolgersi per le tematiche precedentemente trattate dall'utente stesso. Se per esigenze lavorative sorgesse la necessità di accedere al contenuto di tale casella di posta, il Responsabile della struttura organizzativa a cui l'utente era assegnato potrà inoltrare, anche tramite il referente SIRe, motivata richiesta all'Amministratore di sistema.

11.19 In coerenza con il punto 8.8 non è prevista la possibilità di produrre copia delle caselle di posta per utenti non più in servizio presso l'Amministrazione. In ogni caso si informa che il contenuto delle caselle di posta elettronica cancellate potrà essere trattato dall'Ente, per il tramite dell'Amministratore di sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. Le informazioni così raccolte saranno utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento,

che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

Si informa che, ai sensi della normativa sull'archiviazione e conservazione degli atti amministrativi, dell'articolo 2214 del Codice civile e dell'articolo 22 del Dpr 600/73, per ottemperare legittime istanze di accesso agli atti ai sensi della L. 241/90 o accesso civico generalizzato (d.lgs 33/13) l'Ente deve conservare per dieci anni sui propri Server di Posta Elettronica tutti i messaggi di posta elettronica aventi rilevanza istruttoria o inerenti l'attività procedimentale e contrattuale.

L'Ente, per il tramite dell'Amministratore di sistema, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.

12 Processo di abilitazione/disabilitazione alle procedure

12.1 Il Responsabile (Direttore/Dirigente) determina per ogni dipendente assegnato alla Struttura le abilitazioni e i profili da attribuire, modificare o revocare in coerenza con le funzioni e le singole attività per ciascuno di essi secondo le regole di liceità, correttezza e trasparenza, anche con riferimento alle corrette profilazioni sulla base del principio di accountability sancito dal Regolamento (UE) 2016/679. È richiesta pertanto ai responsabili delle strutture regionali una costante verifica di tipo organizzativo sulla necessità e attualità delle abilitazioni in capo ai dipendenti assegnati alla propria struttura.

12.2 I percorsi di abilitazione e disabilitazione devono essere "tracciabili" e veicolati, dal referente Sire Asset, attraverso gli strumenti messi a disposizione dall'Amministrazione, verso il "soggetto individuato"

La responsabilità delle attribuzioni e delle mancate cancellazioni è una responsabilità del dirigente.

12.3 Ogni qualvolta il "soggetto individuato" abiliti un dipendente ad una procedura/applicativo con il relativo profilo, deve essere dato riscontro al dirigente, ai referenti SIRe Asset della direzione e al dipendente abilitato. Si intende per "soggetto individuato" chi detiene la possibilità di attribuire ruoli/profili alle persone rispetto agli applicativi: il ruolo può essere in capo al CSI Piemonte e/o a altri funzionari dell'Ente in relazione allo specifico applicativo.

13 Utilizzo dei telefoni, fotocopiatrici, scanner e stampanti messi a disposizione dall'Ente.

13.1 L'utente è consapevole che tutti gli strumenti dati in uso sono Asset messi a disposizione dall'Ente per lo svolgimento dell'attività lavorativa.

13.2 Qualora venisse assegnato uno smartphone o cellulare, o anche la sola SIM, all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari, smartphone e/o SIM dell'Ente si applicano, a compendio delle regole definite dall'Ufficio competente, le

disposizioni sopra previste per gli altri dispositivi informatici e per l'accesso in rete, per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle indicazioni per la protezione dell'accesso al dispositivo e per il corretto uso della navigazione in Internet e della posta elettronica (cfr. punti 10 e 11).

13.3 La stampa di documenti avviene, di norma, su dispositivi multifunzione disponibili all'interno delle sedi regionali e condivise mediante il dominio *regpient01*.

13.4 Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

a) stampare documenti solo se strettamente necessario per lo svolgimento delle proprie funzioni operative;

b) prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.

13.5 Sia per l'attività in ufficio sia nei casi di telelavoro e lavoro agile non è prevista l'assegnazione di dispositivi di stampa individuali.

13.6 Nel caso in cui si rendesse necessaria la stampa di informazioni riservate, l'utente dovrà utilizzare le apposite funzioni di stampa riservata, disponibili sui dispositivi multifunzione, per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

13.7 Non è consentita l'installazione di dispositivi di stampa di proprietà degli utenti sui PC messi a disposizione dall'Ente

14 Assistenza agli utenti e manutenzioni

14.1 L'Amministratore di sistema può accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

a) verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;

b) verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;

c) richieste di aggiornamento software e manutenzione preventiva hardware e software.

14.2 Gli interventi tecnici possono avvenire previo consenso dell'utente quando l'intervento di che trattasi richiede l'accesso ad aree personali dell'utente stesso.

14.3 L'accesso in teleassistenza sui PC della rete richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

14.4 Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o l'Amministratore di sistema devono presenziare alla sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente disciplinare.

15 LOG di sistema

15.1 I log relativi all'uso del File System di dominio e della intranet, quelli relativi all'utilizzo di strumenti, reperibili nella memoria degli strumenti stessi ovvero sui server o sui router, nonché i file salvati o trattati su Server o strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di sistema, per esigenze di servizio, per la sicurezza del lavoro e per la tutela del patrimonio, ovvero quando la verifica sia conseguente a specifiche richieste delle autorità competenti.

Le informazioni registrate nei log dipendono dalla natura degli eventi tracciati e dalle finalità associate. Devono almeno permettere di:

- Imputare l'evento tracciato (azione o tentativo di azione sul sistema informatico) al proprio autore (persona fisica, attrezzatura tecnica, programma informatico, ecc.).
- Datare l'evento (grazie alla sincronizzazione degli orologi di sistema).
- Valutare l'evento in termini di: tipo di operazione (es. invio di una mail), parametri rilevanti dell'azione (es. destinatari della mail), risultato dell'operazione (es. successo o fallimento).

In nessun caso i messaggi di log possono contenere informazioni confidenziali come password o i corrispondenti hash, qualsiasi forma di autenticazione utente (es. chiavi pubbliche) o altra informazione la cui riservatezza deve essere preservata.

15.2 I controlli possono avvenire secondo le disposizioni previste al successivo punto 16 del presente Regolamento.

15.3 Le informazioni in possesso dell'Amministrazione regionale di cui al comma 1 potranno essere utilizzate, nei limiti di quanto previsto nel presente Disciplinare, per tutti i fini connessi al rapporto di lavoro e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

16 Controlli sugli strumenti informatici (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

16.1 Poiché in caso di violazioni contrattuali e giuridiche, sia il datore di lavoro, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e [...] previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali [...][8], può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori, di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di

8 Cfr. art. 4,comma 1, L. 20 maggio 1970, n.300

modificazione di procedimenti tecnici destinati a controllare i movimenti[9] o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto del presente Disciplinare e dei seguenti principi:

- Proporzionalità: il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi;
- Trasparenza: l'adozione del presente Disciplinare ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti;
- Pertinenza e non eccedenza: ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

16.2 L'uso degli strumenti informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato al precedente punto 15 del presente Disciplinare. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti ai punti 17 e 18) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti informatici.

17 Controlli per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, ecc.).

17.1 Qualora, per le finalità qui sopra descritte, risulti necessario l'accesso agli strumenti e alle risorse informatiche e relative informazioni descritte al punto 6, 7, 8, 10 e 11, l'Amministratore di sistema si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

i Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Disciplinare.

ii Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare l'Amministratore di sistema, potendo così accedere alle informazioni descritte al punto 15 con possibilità di rilevare file trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo dell'indirizzo IP dell'utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.

9 Vale disposto art. 4, comma 2, L.300/1970

iii Qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti i. e ii., l'Amministratore di sistema potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale sottoscritto dall'Amministratore di sistema che ha svolto l'attività.

In caso di nuovo accesso da parte dell'utente allo Strumento informatico oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche).

18 Conservazione dei dati

18.1 In riferimento agli articoli 5 e 6 del Reg. 679/16 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e al traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, sono mantenute per 180 giorni dalla loro produzione.

18.2 In casi eccezionali – ad esempio: per esigenze tecniche o di sicurezza o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria – è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.

18.3 L'Ente si impegna ad applicare le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

Le misure di sicurezza implementate per proteggere i log, da problemi operativi o modifiche non autorizzate (volontarie o involontarie) garantiscono:

- la correttezza dei messaggi di log, sottoponendo a controllo i meccanismi di generazione dei log per ogni sistema IT;
- l'integrità dei messaggi di log, mediante meccanismi di cifratura durante la trasmissione degli stessi dalla fonte alla piattaforma di centralizzazione;
- la disponibilità dei messaggi di log: grazie a meccanismi di fault tolerance relativi al dimensionamento della memoria delle fonti di log;
- l'inalterabilità e l'accesso autorizzato ai messaggi di log: secondo il principio di Segregation of Duties e tramite meccanismi di controllo accessi alla piattaforma, consentiti solamente da rete IT;
- sul file system centralizzato, i log sono raccolti solo per la finalità di conservazione, secondo quanto stabilito dalle vigenti Leggi;
- l'accesso è consentito solo alle PDL degli specialisti di sicurezza.

19 Utilizzo dei Social Network

19.1 L'utilizzo a fini promozionali e commerciali di strumenti di tipo "social media", dei blog e dei forum, anche professionali, è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive e istruzioni operative al personale addetto alla comunicazione attraverso gli account istituzionali.

19.2 La partecipazione o consultazione dei social media durante l'orario di lavoro è consentita esclusivamente in casi di necessità lavorative o necessità di contatti attraverso messaggistica istantanea.

19.3 Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, quanto i propri collaboratori, oltre che gli stessi utenti utilizzatori dei social media.

19.4 Il presente articolo deve essere osservato dall'utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.

19.5 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione di competenza.

19.6 L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso scritto di questi, e comunque non potrà "postare" nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso scritto/esplicito del Responsabile della Struttura di appartenenza , salvo in casi di manifestazioni pubbliche ad accesso libero.

19.7 Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

20 Pubblicazione e messa a disposizione

20.1 Il presente Disciplinare è stato redatto dal Gruppo di lavoro interdirezionale GDPR con il supporto del Responsabile per la protezione dei dati che è chiamato a garantire il coordinamento degli adempimenti.

20.2 La sua pubblicizzazione avverrà nelle seguenti forme: trasmissione per posta elettronica interna a tutti i Responsabili di Struttura e a tutti gli utenti, attraverso la intranet della Giunta regionale.

21 Sanzioni disciplinari

21.1 È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con il presente disciplinare.

21.2 L'inosservanza di quanto disposto nel presente documento dà luogo a responsabilità disciplinare qualora rientri in una delle infrazioni previste dal codice disciplinare.