erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

REGOLAMENTO PER LA DISCIPLINA DEL LAVORO AGILE

Art. 1
Premessa e riferimenti normativi

1. Il presente regolamento disciplina l'applicazione del lavoro agile ordinario (anche denominato "smart working") al personale di ERAP Marche definendone ambiti di attivazione, modalità di esecuzione e limiti di accesso, nel rispetto dei seguenti riferimenti normativi:

- Legge 7 agosto 2015, n. 124 "Deleghe al Governo in materia di riorganizzazione delle Amministrazioni pubbliche" art. 14, come modificato dalla Legge n. 27/2020 art. 87-bis co. 5 e dalla Legge n. 77/2020 art. 263 co. 4-bis;
- Legge 22 maggio 2017, n. 81 "Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato", Capo II "Lavoro Agile";
- Decreto-legge 17 marzo 2020, n. 18, convertito con modificazioni in Legge n. 27/2020, art. 87;
- Direttiva della Presidenza del Consiglio dei Ministri 4 maggio 2020 n. 3 recante "Modalità di svolgimento della prestazione lavorativa nell'evolversi della situazione epidemiologica da parte delle pubbliche amministrazioni"
- Decreto-legge 19 maggio 2020, n. 34, convertito con modificazioni in Legge 77/2020, art. 263;
- DPCM del 23 settembre 2021 (decreto rientro in presenza) in attuazione dell'art. 87 comma 1 del DL. n. 18 del 17 marzo 2020 convertito con modificazioni dalla legge 24 aprile 2020 n. 27.
- DM dell'8 ottobre 2021crelativo alle "Modalità organizzative per il rientro in presenza dei lavoratori delle pubbliche amministrazioni";
- art. 6 del D.L. 9 giugno 2021 n. 80, convertito nella legge 6 agosto 2021 n. 113.
- CCNL – relativo al comparto delle funzioni locali – triennio 2019 / 2022 sottoscritto in data 16.11.2022, artt. 63 e ss.
- Delibera CdA n. 275/2021 del 29.11.2021 (Modalità di lavoro agile. Adeguamento alle prescrizioni del D.P.C.M. 23 settembre 2021 e del decreto della Presidenza del Consiglio dei ministri, Dipartimento della funzione pubblica, dell'8 ottobre 2021, pubblicato in G.U. 13 ottobre 2021, n. 245)
- Delibera CdA n. 315/2021 del 28.12.2021 (integrazione delibera CdA n. 275/2021relativa allo svolgimento della prestazione lavorativa in modalità agile)
- Delibera CdA n. 27/2023 del 30.01.2023 (approvazione PIAO 2023 – 2025) - sezione 4.2 "Lavoro Agile

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

Art. 2
Definizioni e finalità

1. Ai fini del presente regolamento si intende per "*Lavoro agile*" una modalità flessibile di esecuzione del rapporto di lavoro connotata da un'organizzazione delle attività per cicli, fasi e obiettivi e dallo svolgimento di parte dell'attività all'esterno della sede lavorativa senza vincoli di spazio e di orario, entro i soli limiti di durata del tempo di lavoro giornaliero e settimanale derivanti dalla legge e dalla contrattazione collettiva, e nel rispetto della fascia di contattabilità di cui all'art. 7, comma 5 del presente Regolamento.
2. Il lavoro agile risponde alle seguenti finalità:
   a) sperimentare ed introdurre nuove soluzioni organizzative che favoriscano lo sviluppo di una cultura gestionale orientata al lavoro per obiettivi e risultati e, al tempo stesso, ad un incremento di produttività;
   b) favorire un'organizzazione ispirata a principi di flessibilità, autonomia e responsabilità e fondata su legami di fiducia, nell'ottica del superamento della logica del mero controllo visivo;
   c) favorire la digitalizzazione e la dematerializzazione delle attività, dei processi e dei procedimenti, garantendo comunque il miglior impatto per l'utenza in termini di accessibilità, anche da remoto, ai servizi erogati dalle strutture regionali;
   d) rafforzare le misure di conciliazione dei tempi di vita - lavoro dei dipendenti;
   e) promuovere la mobilità sostenibile tramite la riduzione degli spostamenti casa-lavoro nell'ottica di una politica ambientale sensibile alla diminuzione del traffico urbano in termini di volumi e di percorrenze;
   f) contribuire alla razionalizzazione nell'utilizzo degli spazi, delle sedi di lavoro e delle dotazioni tecnologiche realizzando economie di gestione.

Art. 3
Destinatari

1. Il lavoro agile si applica a tutto il personale dipendente di ERAP Marche che svolge la propria prestazione nell'ambito di un rapporto di lavoro subordinato a tempo indeterminato o determinato, pieno o parziale, nel rispetto del principio di non discriminazione e nella percentuale massima del 30% del personale di ogni servizio. Costituiscono tuttavia eccezione i dipendenti che, nello svolgimento della prestazione lavorativa, richiedono una modalità di lavoro in presenza.
2. Per il personale nuovo assunto a tempo indeterminato o determinato e/o a tempo parziale l'applicazione del lavoro agile va coordinata con l'esperienza lavorativa acquisita; il dirigente valuta

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

se autorizzare la modalità smart working prima del termine del periodo di prova previsto contrattualmente.

3. Il personale in posizione di comando o distacco in uscita può svolgere la prestazione lavorativa in modalità agile secondo la disciplina organizzativa prevista nell'ente ove svolge concreto servizio. Analogamente, il personale dipendente in posizione di comando o distacco in entrata effettua domanda sulla base del presente regolamento, in accordo con i dirigenti responsabili della struttura provinciale in cui presta temporaneamente servizio.
4. La prestazione lavorativa in modalità agile è autorizzata dal Responsabile del Presidio previo parere non vincolante del Responsabile del Servizio di appartenenza in merito alla possibilità di svolgimento della prestazione lavorativa in modalità agile senza pregiudizio per l'organizzazione del servizio. Il Responsabile di Presidio in particolari circostanze può elevare la percentuale di cui al comma 1.

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

1. Il lavoro agile ha natura consensuale e volontaria e si realizza all'interno del rapporto di lavoro in corso con il mantenimento sia della struttura di assegnazione che della posizione giuridico-economica. Per accedere alla modalità di lavoro agile i dipendenti dichiarano:
   - di saper utilizzare i software gestionali in uso in Erap Marche, relativamente al proprio ambito lavorativo/settore di riferimento;
   - di conoscere le modalità operative del lavoro agile, come da documentazione reperibile sulla sezione "Smart Working – Manuali e Linee guida";
   - di aver preso visione delle disposizioni normative in materia di salute e sicurezza sui luoghi di lavoro e policy per la sicurezza informatica che si allegano al presente Regolamento (Allegati all'Accordo individuale: "Tutela della Salute e della Sicurezza del personale in Lavoro Agile" e "Policy per la sicurezza informatica e per l'utilizzo degli strumenti informativi e telematici").
2. L'attivazione del lavoro agile ha carattere volontario. Il dipendente interessato presenta specifica richiesta compilando il modulo disponibile sulla sezione del sito di ERAP Marche – modulistica denominato "Accordo individuale di lavoro agile". Lo svolgimento della prestazione lavorativa in modalità agile viene autorizzata dal Dirigente Responsabile del presidio, previo parere del Dirigente del Servizio di appartenenza, mediante sottoscrizione del relativo accordo.
3. Il dirigente Responsabile del Presidio nell'autorizzare lo svolgimento del lavoro agile, tiene conto dei seguenti requisiti di ammissibilità:
   a) garantire l'invarianza dei servizi resi all'utenza;
   b) prevedere un'adeguata rotazione del personale autorizzato al lavoro agile, assicurando la prevalenza del lavoro in presenza di ciascuno;
   c) non avere lavoro arretrato accumulato, ancora da smaltire e, qualora ce ne sia, predisporre un idoneo e documentabile piano di smaltimento;
   d) tener conto della mappatura delle attività che possono essere rese in modalità agile, già effettuata

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

da ciascun dirigente e pubblicata sul sito internet di Erap Marche nella sezione "___" – smart working (documento "Mappatura delle attività").

4. In considerazione della natura flessibile del lavoro agile, fermo restando il possesso dei requisiti di cui al punto 3, rilevano le priorità previste dall'art. 18 comma 3-bis della Legge n. 81/2017 e s.m.i., e nello specifico:
   a) dipendenti con figli fino a dodici anni di età o senza alcun limite di età nel caso di figli in condizioni di disabilità ai sensi dell'articolo 3, comma 3, della legge 5 febbraio 1992, n. 104;
   b) dipendenti con disabilità in situazione di gravità accertata ai sensi dell'articolo 4, comma 1, della legge 5 febbraio 1992, n. 104 o che siano caregivers ai sensi dell'articolo 1, comma 255, della legge 27 dicembre 2017, n. 205;
5. La lavoratrice o il lavoratore che richiede di fruire del lavoro agile non può essere sanzionato, demansionato, licenziato, trasferito o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro. Qualunque misura adottata in violazione del precedente periodo è da considerarsi ritorsiva o discriminatoria e, pertanto, nulla.
6. Subordinatamente alle priorità di cui al comma 4 del presente articolo, assumono carattere prioritario le richieste di esecuzione del rapporto in modalità agile formulate:
   (1) dai dipendenti con figli in condizioni di disabilità ai sensi dell'art. 3, comma 3, della legge 5 febbraio 1992, n. 104;
   (2) dai dipendenti disabili nelle condizioni di cui all'art. 3, comma 3, della legge 5 febbraio 1992, n. 104 o che abbiano nel proprio nucleo familiare una persona con disabilità nelle condizioni di cui all'art. 3, comma 3, della legge n. 104/1992, lavoratori immunodepressi e familiari conviventi di persone immunodepresse;
   (3) dai lavoratoti residenti o domiciliati in comuni che distano dalla sede di lavoro più di km. 50;
   (4) dalla lavoratrice in stato di gravidanza;
   (5) dai dipendenti nei tre anni successivi alla conclusione del periodo di congedo di maternità;
   (6) dai lavoratori con figli conviventi nel medesimo nucleo familiare minori di anni tre;
   (7) dai lavoratori con figli conviventi nel medesimo nucleo familiare minori di quattordici anni.

Art. 5
Trattamento giuridico ed economico

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

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

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

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

Art. 6
Accordo individuale di lavoro

1. L'accordo individuale di smart working di cui al precedente art. 4, comma 2, redatto per iscritto sulla base del modello di cui all'allegato A al presente Regolamento, consiste in un accordo tra le parti contenente le modalità e le condizioni di svolgimento del lavoro agile.
2. L'Accordo individuale di lavoro nello specifico prevede:
   a) le attività da espletare e obiettivi da conseguire in lavoro agile, tenuto conto delle attività di cui al precedente art. 4, comma 3, lett. d);
   b) la strumentazione tecnologica necessaria allo svolgimento dell'attività lavorativa fuori dalla sede di lavoro;
   c) la decorrenza della modalità agile che coincide con il primo giorno del mese successivo a quello in cui è avvenuta l'autorizzazione da parte del dirigente, ai sensi dell'art. 4, comma 2 ultimo periodo del presente Regolamento;
   d) la durata dell'attività da svolgere in modalità agile determinata in un periodo di massimo di un anno. In fase di prima applicazione, la scadenza è fissata per tutti al 31.12.2023
   e) gli obblighi connessi all'espletamento dell'attività in modalità agile e le forme di esercizio del potere direttivo e di controllo del datore di lavoro sulla prestazione resa dal lavoratore all'esterno dei locali dell'amministrazione, nel rispetto di quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300 e s.m.i.;
   f) l'indicazione delle giornate di lavoro da svolgere a distanza;
   g) le fasce di contattabilità, i tempi di disconnessione con le fasce di inoperabilità;
   h) il luogo prescelto in via prevalente per l'esecuzione della prestazione lavorativa fuori dai locali aziendali;
   i) le modalità di cessazione;
   j) l'impegno del lavoratore a rispettare le prescrizioni indicate nell'informativa sulla salute e sicurezza

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

sul lavoro agile, ricevuta dall'amministrazione;

k) le modalità con cui il datore di lavoro esercita il potere direttivo, di controllo e disciplinare;

All'accordo individuale sono allegati, costituendone parte integrante:

– l'informativa in materia di tutela della salute e sicurezza del personale in lavoro agile (Allegato B).

– le prescrizioni in materia di sicurezza informatica e utilizzo degli strumenti informativi e telematici (Allegato C).

Al fine di consentire l'adeguamento nel tempo dell'accordo individuale esso potrà essere rinnovato/integrato per la parte concernente le attività e i risultati da raggiungere, attraverso la compilazione di apposito modulo denominato "Accordo integrativo smart working". Tale modulo ripropone l'intero Accordo Individuale ed è modificabile esclusivamente per i campi relativi alle attività e agli obiettivi da raggiungere, nonché alla strumentazione informatica.

Qualora, in corso di vigenza dell'accordo, il dipendente cambi Servizio di assegnazione giuridica o lavorativa, l'accordo in essere cessa d'ufficio e occorre procedere alla sottoscrizione di un nuovo Accordo Individuale; lo stesso vale anche nel caso di modifica del contratto di lavoro (trasformazione da full time a part-time o viceversa, da part-time orizzontale a part-time verticale, progressione di carriera, comandi parziali in entrata/in uscita). Non occorre invece procedere ad un nuovo accordo nel caso in cui cambia il Dirigente responsabile, ma resta inalterata la struttura di assegnazione.

Art. 7
Modalità di esecuzione della prestazione e orario di lavoro

1. L'attuazione del lavoro agile non modifica la regolamentazione dell'orario di lavoro applicata al dipendente, il quale farà riferimento al "normale orario di lavoro" (full-time o part-time) con le caratteristiche di flessibilità temporali proprie del lavoro agile nel rispetto, comunque, dei limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione.
2. Nell'ambito dello svolgimento della prestazione lavorativa possono essere individuate:

a) per i dipendenti 2 giornate la settimana di lavoro in modalità agile, assicurando comunque la prevalenza settimanale di lavoro in presenza; In caso di rapporto di lavoro a tempo parziale verticale e comando/distacchi, le giornate vengono riproporzionate. Resta garantita l'ampia flessibilità basata su un rapporto consapevole e di fiducia tra le parti e la possibilità di variare – anche temporaneamente e senza necessità di modifica formale dell'accordo - l'articolazione delle giornate su base mensile per esigenze organizzative e/o personali, sempre . 11 rispettando la prevalenza delle giornate di lavoro in presenza. In tal senso la variazione viene concordata con il dirigente e la

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

Posizione Organizzativa di riferimento, e giustificata tramite specifico giustificativo web entro le 24 ore antecedenti, all'interno del mese in corso; in ogni caso i giorni di lavoro agile non fruiti non sono recuperabili nel mese successivo.

b) per i titolari di posizione organizzativa, ora incaricati di elevate qualificazioni, tenuto conto del ruolo e delle deleghe dirigenziali attribuite, ferme restando le condizioni di cui all'art. 5 c. 2 lett. c), di norma una giornata di lavoro agile alla settimana al fine di garantire l'efficace coordinamento dell'area, salvo motivata richiesta derogatoria;

c) c) per i dirigenti tenuto conto del ruolo e ferme restando le condizioni di cui all'art. 5 c. 2 lett. c), una giornata di lavoro agile alla settimana al fine di garantire l'efficace coordinamento del Settore a cui sono preposti;

3. Ai fini della verifica del rispetto dell'orario di lavoro, la giornata di lavoro agile è considerata equivalente a quella svolta presso la sede di servizio· Fatte salve le fasce di contattabilità di cui al successivo punto 5, al dipendente in lavoroagile è garantito il rispetto dei tempi di riposo nonché il "diritto alla disconnessione" dalle strumentazioni tecnologiche.

1. Nello specifico, nelle giornate di lavoro agile, per il dipendente valgono le seguenti regole:
2. fascia di contattabilità: Tale fascia oraria non può essere superiore all'orario medio giornaliero di lavoro ed è articolata anche in modo funzionale a garantire le esigenze di conciliazione vita-lavoro del dipendente. Per la giornata senza rientro corrisponde all'orario 9:00-13.00, e per la giornata con rientro corrisponde all'orario 9.00-13.00 e 15:30-17.00, da riproporzionare in caso di part-time. Il lavoratore in questa fascia è contattabile sia telefonicamente che via mail o con altre modalità similari
3. fascia di attività: all'interno della fascia 07:30 – 19:00, fatte salve le fasce di contattabilità di cui al punto precedente, il dipendente organizza autonomamente la propria prestazione lavorativa con riferimento al proprio orario teorico giornaliero e agli obiettivi assegnati
4. fascia di inoperabilità (disconnessione): 19.00 – 7:30; nella quale il lavoratore non può erogare alcuna prestazione lavorativa. né può essere contattato telefonicamente, o via mail o con altre modalità similari. Tale fascia comprende il periodo di 11 ore di riposo consecutivo di cui all'art. 29, comma 6, del CCNL Comparto Funzioni locali 2019-2021 a cui il lavoratore è tenuto
5. Nella fascia di contattabilità, il dipendente può richiedere, ove ne ricorrano i relativi presupposti. la fruizione dei permessi previsti dal CCNL o dalle norme di legge quali, a titolo esemplificativo, i permessi per particolari motivi personali o familiari, i permessi sindacali di cui al CCNQ 4 dicembre 2017 e s.m.i., i permessi di cui all'art. 33 della legge 104/1992. Il dipendente che fruisce dei suddetti permessi, per la durata degli stessi, è sollevato dagli obblighi stabiliti dal comma precedente per le fasce di contattabilità.
4. Nelle giornate in cui la prestazione lavorativa viene svolta in modalità agile non è possibile effettuare lavoro straordinario, trasferte, lavoro disagiato, lavoro svolto in condizioni di rischio.
5. In caso di problematiche di natura tecnica e/o informatica, e comunque in ogni caso di cattivo

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

funzionamento dei sistemi informatici, qualora lo svolgimento dell'attività lavorativa a distanza sia impedito, reso non sicuro o sensibilmente rallentato, il dipendente è tenuto a darne tempestiva informazione al proprio dirigente. Lo stesso può richiamare il dipendente a lavorare in presenza. In caso di ripresa del lavoro in presenza, si applica la disciplina di cui ai successivi.

6. Per sopravvenute e documentate esigenze di servizio il dirigente può richiamare in sede il dipendente, dandone comunicazione almeno il giorno prima, tenendo conto della fascia di inoperabilità.
7. Nei casi eccezionali in cui il dirigente, con apposita motivazione, richiede che il dipendente rientri in sede per motivi di servizio, senza che sia possibile rispettare il preavviso di cui al comma 8, il dipendente accede alla sede di lavoro previa timbratura. In questo caso si applica la disciplina relativa al lavoro svolto presso la sede di lavoro. In alternativa, il dipendente può decidere di non completare l'orario in presenza e proseguire la giornata in modalità lavoro agile come da calendario. In questo caso, le timbrature rilevano ai soli fini della sicurezza.

Art. 8
Dotazione Tecnologica e Sicurezza dei dati

6. L'Amministrazione mette di norma a disposizione l'attrezzatura tecnologica adatta e necessaria per lo svolgimento della prestazione lavorativa in lavoro agile, sulla base di specifiche mansioni da svolgere. A livello indicativo, la strumentazione completa è costituita da: un pc portatile e/o dispositivo equipollente comprensivo degli applicativi software utilizzati, corredati dagli accessori necessari per un corretto funzionamento e una adeguata fruizione della tecnologia necessaria allo svolgimento delle mansioni.
7. Il personale si impegna a custodire con la massima cura e mantenere integra la strumentazione che viene fornita, in modo tale da evitarne il danneggiamento, lo smarrimento e a utilizzarla in conformità con le istruzioni ricevute (Allegato C "Policy per la sicurezza informatica e per l'utilizzo degli strumenti informativi e telematici").
8. Al fine di ottimizzare la gestione delle attrezzature tecnologiche disponibili e l'utilizzo delle stesse in modalità lavoro agile, l'Amministrazione prevede alla progressiva implementazione delle postazioni informatiche di lavoro con dispositivi portatili, che sarà completata nell'arco di un quinquennio.
9. Nel frattempo, qualora la strumentazione idonea da fornire, o parte di essa, non sia disponibile, il dipendente espleta la propria prestazione lavorativa in modalità agile avvalendosi di supporti informatici di sua proprietà o nella sua disponibilità; in tal caso viene garantita, su richiesta del dipendente, la verifica da parte del referente informatico di riferimento, della configurazione delle

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

impostazioni che eventualmente impediscono il corretto utilizzo dei sistemi informativi messi a disposizione dall'Amministrazione.

10. L'accesso alle risorse digitali e alle applicazioni raggiungibili tramite la rete internet avviene attraverso il sistema di gestione di identità digitale "_____" in grado di assicurare un livello di sicurezza adeguato. Qualora, si renda necessario accedere ai server contenenti applicativi, database o sistemi non fruibili tramite browser, l'Amministrazione autorizza l'accesso alle risorse attraverso VPN (Virtual Private Network), previa verifica da parte del dirigente e del referente informatico e relativa comunicazione al Servizio competente in materia di sistemi informatici.
11. I costi sostenuti dal dipendente direttamente e/o indirettamente collegati allo svolgimento della prestazione lavorativa (elettricità, linea di connessione, etc.) o le eventuali spese per il mantenimento in efficienza dell'ambiente di lavoro agile non sono a carico dell'Amministrazione.
12. Eventuali impedimenti tecnici (come malfunzionamenti della linea dati o problemi di comunicazione telefonica) allo svolgimento dell'attività lavorativa nelle giornate di lavoro agile devono essere tempestivamente comunicati dal dipendente al dirigente e al proprio referente informatico al fine di dare rapida soluzione al problema. Qualora ciò non sia possibile, vanno concordate con il dirigente responsabile le modalità di completamento della prestazione, ivi compreso, ove possibile, il rientro del dipendente nella sede di lavoro, alle condizioni di cui al precedente articolo.
13. Alla postazione di lavoro agile sono applicati i normali protocolli di sicurezza previsti nell'ambito dei piani per il trattamento dei dati e per la salvaguardia della loro integrità e riservatezza, nel rispetto di standard di sicurezza equivalenti a quelli garantiti alle postazioni lavorative presenti nei Presidi provinciali. Il dipendente in lavoro agile è tenuto al rispetto della normativa inerente il segreto d'ufficio e della normativa inerente la protezione dei dati personali di cui al decreto legislativo n. 196 del 2003 e al Reg.UE n. 679/2016, nonché a quanto stabilito nell'allegato ___ al presente Regolamento.

Art. 9
Formazione

1. Per agevolare ed ottimizzare l'utilizzo del lavoro agile, il Piano formativo prevede appositi percorsi formativi in materia di: modalità operative del lavoro agile, utilizzo delle piattaforme di comunicazione, dei principali applicativi gestionali dell'Ente, e quant'altro si renda necessario al fine di incentivare l'innovazione organizzativa e la modernizzazione dei processi di lavoro richiesti dal lavoro agile.
2. L'Amministrazione garantisce ai dipendenti che svolgono il lavoro in modalità agile le stesse opportunità formative, finalizzate al mantenimento e allo sviluppo della professionalità, previste per tutti i dipendenti che svolgono mansioni analoghe

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

3. Al fine di aumentare l'efficacia e l'efficienza della prestazione svolta in smart working, il dirigente può disporre per il dipendente la partecipazione a formazione *ad hoc*.

Art. 10
Sicurezza sul lavoro

1. Il lavoratore che svolge la propria prestazione lavorativa in modalità smart working, sulla base della formazione ricevuta, nel rispetto dei requisiti di cui al presente regolamento, delle previsioni di cui all'informativa di cui all'allegato __ del presente Regolamento, è tenuto a rispettare ed 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. L'Amministrazione, ai sensi dell'art. 22, comma 1 della Legge n. 81/2017, garantisce la salute e la sicurezza del lavoratore che svolge la prestazione in modalità di lavoro agile.

Art. 11
Assicurazione obbligatoria per gli infortuni e le malattie professionali

1. Il lavoratore ha diritto alla tutela contro le malattie professionali e gli infortuni sul lavoro dipendenti da rischi connessi alla prestazione lavorativa resa all'esterno dei locali aziendali.
2. La tutela viene garantita anche per malattie e infortuni occorsi durante il percorso di andata e ritorno tra l'abitazione e il luogo di lavoro prescelto, nei termini indicati nell'Accordo individuale.

Art. 12
Valutazione e monitoraggio

1. L'attività svolta in modalità agile e i risultati raggiunti, analogamente a quanto previsto per l'attività lavorativa prestata in sede, sono rendicontate in apposita scheda inviata al dirigente e sono inoltre oggetto di valutazione nell'ambito del sistema di misurazione e valutazione della performance organizzativa e individuale vigente nell'Amministrazione.
2. Nel valutare la prestazione del dipendente resa in modalità agile, il dirigente tiene conto delle attività e dei risultati in relazione agli obiettivi indicati nell'Accordo individuale nel rispetto di quanto previsto dall'art. 6, comma 2.
3. Nel valutare la prestazione si tiene conto di comportamenti e competenze rilevanti quali, a titolo esemplificativo, responsabilità, autoorganizzazione/autonomia, comunicazione, orientamento al risultato, "*problem solving*", lavoro di gruppo, capacità e tempi di risposta e orientamento all'utenza.
4. I dirigenti monitorano l'attività prestata dal dipendente e il raggiungimento dei risultati attesi, anche

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

confrontandosi con il dipendente stesso per condividere punti di forza e di debolezza e risolvere eventuali problematiche.

Art. 13
Cessazione anticipata

1. Il lavoratore agile e l'Amministrazione possono recedere dall'Accordo di lavoro agile in qualsiasi momento con un preavviso di almeno 15 giorni.
2. Nel caso di lavoratore agile disabile ai sensi dell'art. 1 della legge 12 marzo 1999, n. 68, il termine del preavviso del recesso da parte dell'Amministrazione non può essere inferiore a 30 giorni, al fine di consentire un'adeguata riorganizzazione dei percorsi di lavoro rispetto alle esigenze di vita e di cura del lavoratore. In presenza di un giustificato motivo, ciascuno dei contraenti può recedere prima della scadenza del termine nel caso di Accordo a tempo determinato.
3. L'Accordo individuale di lavoro agile può, in ogni caso, essere revocato dal Dirigente Responsabile del Presidio nel caso:
a) in cui il dipendente non rispetti i tempi o le modalità di effettuazione della prestazione lavorativa, la corretta rendicontazione delle attività o in caso di ripetuto mancato rispetto delle fasce di contattabilità;
b) di mancato raggiungimento degli obiettivi assegnati;
c) di mutate esigenze organizzative del servizio.
4. In caso di revoca il dipendente è tenuto a riprendere la propria prestazione lavorativa secondo l'orario ordinario presso la sede di lavoro entro il termine previsto dalla comunicazione della revoca che potrà avvenire per e-mail ordinaria personale e/o per PEC con un preavviso minimo di 7 giorni. L'avvenuto recesso o revoca dell'Accordo individuale è comunicato dal Dirigente del Servizio al Responsabile del Servizio Personale.
5. In caso di trasferimento del dipendente ad altro Servizio – Presidio l'accordo individuale cessa di avere efficacia dalla data di effettivo trasferimento del lavoratore.

Art. 14
Lavoro agile e personale con qualifica dirigenziale

1. Al personale dirigenziale, come per quello del comparto, è consentita la possibilità di svolgere attività lavorativa in modalità agile, assicurando il prevalente svolgimento in presenza della prestazione.
2. Si applicano al personale con qualifica dirigenziale le disposizioni contenute nel presente regolamento laddove compatibili.

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

Piazza Salvo d'Acquisto n° 40
60131 Ancona
tel. (071) 28531 – fax (071) 2867028
pec: erap.marche@emarche.it

3. La prestazione lavorativa in modalità agile, analogamente a quella prestata in sede, è oggetto di valutazione nell'ambito degli obiettivi di performance annuali individuati all'interno del Piano Integrato di Attività e Organizzazione (PIAO) sezione 4.2 "lavoro agile". L'Accordo individuale per la prestazione di lavoro agile del personale dirigente è autorizzato dal Responsabile del Presidio e per il Responsabile del Presidio l'autorizzazione è a cura del Consiglio di Amministrazione

Art. 15
Disposizioni finali

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

Art. 16
Entrata in vigore

Il presente Regolamento entra in vigore dalla data di esecutività della deliberazione che lo approva.

ACCORDO INDIVIDUALE PER LA PRESTAZIONE IN LAVORO AGILE

La/Il sottoscritta/o _____ dipendente di ERAP Marche, Servizio _____ del Presidio di _____ (C.F _____) e il sottoscritto _____ Dirigente Responsabile del Presidio di _____ dichiarano di ben conoscere e accettare la Disciplina per il lavoro agile approvata dal CdA in data 30.11.2023 con delibera n. _____

CONVENGONO

1. Oggetto

che il/la dipendente è ammesso/a a svolgere la prestazione lavorativa in modalità agile nei termini e alle condizioni di seguito indicate e in conformità alle prescrizioni stabilite nella normativa vigente stabilendo altresì:

- la data di avvio della prestazione di lavoro agile:

_____;

- la data di fine della prestazione lavoro agile:

_____;

- il/i giorno/i settimanale/i per la prestazione in modalità agile

_____;

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

a) fornita dall'Amministrazione:

□ pc portatile

□ monitor

□ cuffie con microfono

□ tastiera

□ mouse

□ altro (specificare)_____

o, in alternativa b) di proprietà/in utilizzo del/della dipendente:

□ pc

□ monitor

□ cuffie con microfono

□ tastiera

□ mouse

□ altro (specificare)_____

Il dipendente si impegna a dare tempestiva comunicazione dell'eventuale malfunzionamento delle dotazioni tecnologiche che renda impossibile la prestazione lavorativa in modalità agile sia al fine di dare soluzione al problema che di concordare con il proprio responsabile le modalità di completamento della prestazione, ivi compreso, ove possibile, il rientro nella sede di lavoro.

2. Luogo di lavoro

_____.

3. Fascia di contattabilità

La fascia di contattabilità obbligatoria del dipendente è individuata nella mattina dalle ore ___ alle ore _____e, in caso di giornata con rientro pomeridiano, dalle ore _____ alle ore _____.

4. Fascia di disconnessione

La fascia di disconnessione è individuata dalle ore _____ alle ore _____, dalle ore 19:00 di tutti i giorni, oltre al sabato, domenica e festivi.

5. Potere direttivo, di controllo e disciplinare

La modalità di lavoro agile non modifica il potere direttivo e di controllo del Datore di lavoro, che sarà esercitato con modalità analoghe a quelle applicate con riferimento alla prestazione resa presso i locali aziendali.

Il potere di controllo sulla prestazione resa al di fuori dei locali aziendali si espliciterà, di massima, attraverso la verifica dei risultati ottenuti.

Tra dipendente in lavoro agile e diretto responsabile saranno condivisi, in coerenza con il Piano della Performance, obiettivi puntuali, chiari e misurabili che possano consentire di monitorare i risultati dalla prestazione lavorativa in lavoro agile. Tali obiettivi saranno indicati mediante progetti che il Dirigente di appartenenza o il Responsabile del Presidio assegnerà e indicherà in apposite schede di lavoro. Per assicurare il buon andamento delle attività e degli obiettivi:

(a) il dipendente e il dirigente responsabile del servizio _____ si confronteranno almeno con cadenza settimanale sullo stato delle attività;

(b) il dipendente rendiconterà le attività svolte nel mese entro il primo giorno del mese successivo mediante compilazione di apposita scheda;

(c) il dirigente responsabile del servizio di appartenenza validerà le schede di rendicontazione inviandole al Responsabile del Presidio entro il 10 di ogni mese.

Restano ferme le ordinarie modalità di valutazione delle prestazioni, secondo il sistema vigente per tutti i dipendenti.

Nello svolgimento della prestazione lavorativa in modalità lavoro agile il comportamento del/della dipendente dovrà essere sempre improntato a principi di correttezza e buona fede e la prestazione dovrà essere svolta sulla base di quanto previsto dai CCNL vigenti e di quanto indicato nel Codice di comportamento. Le parti si danno atto che, secondo la loro gravità e nel rispetto della disciplina legale e contrattuale vigente, le condotte connesse all'esecuzione della prestazione lavorativa all'esterno dei locali aziendali danno luogo all'applicazione di sanzioni disciplinari, così come individuate nel regolamento disciplinare qualora risultanti in contrasto con le disposizioni comportamentali.

Il mancato rispetto delle disposizioni previste dal presente Accordo può comportare l'esclusione da un eventuale rinnovo dell'Accordo individuale; è escluso il rinnovo in caso di revoca disposta ai sensi del successivo art. 6.

Il dipendente si impegna al rispetto di quanto previsto nell'Informativa sulla salute e sicurezza nel lavoro agile di cui, con la sottoscrizione del presente Accordo, conferma di avere preso visione.

6. Recesso e revoca dall'Accordo

Il presente Accordo è a tempo determinato.

Ai sensi dell'art. 19 della legge 22 maggio 2017, n. 81, il lavoratore agile e l'Amministrazione possono recedere dall'Accordo di lavoro agile in qualsiasi momento con un preavviso di almeno un giorno.

Nel caso di lavoratore agile disabile ai sensi dell'art. 1 della legge 12 marzo 1999, n. 68, il termine del preavviso del recesso da parte dell'Amministrazione non può essere inferiore a 30 giorni, al fine di consentire un'adeguata riorganizzazione dei percorsi di lavoro rispetto alle esigenze di vita e di cura del lavoratore. In presenza di un giustificato motivo, ciascuno dei contraenti può recedere prima della scadenza del termine nel caso di Accordo a tempo determinato.

L'Accordo individuale di lavoro agile può, in ogni caso, essere revocato dal Dirigente Responsabile del Presidio nel caso:

a) in cui il dipendente non rispetti i tempi o le modalità di effettuazione della prestazione lavorativa, la corretta rendicontazione delle attività o in caso di ripetuto mancato rispetto delle fasce di contattabilità;

b) di mancato raggiungimento degli obiettivi assegnati;

c) di mutate esigenze organizzative del servizio.

In caso di revoca il dipendente è tenuto a riprendere la propria prestazione lavorativa secondo l'orario ordinario presso la sede di lavoro dal giorno successivo alla comunicazione della revoca. La comunicazione della revoca potrà avvenire per e-mail ordinaria personale e/o per PEC.

L'avvenuto recesso o revoca dell'Accordo individuale è comunicato dal Dirigente/Responsabile al Servizio Personale.
In caso di trasferimento del dipendente ad altro settore/dipartimento, l'Accordo
individuale cessa di avere efficacia dalla data di effettivo trasferimento del lavoratore.

7. Presenza in sede

L'Amministrazione si riserva di richiedere la presenza in sede del dipendente in qualsiasi momento – e in deroga alla pianificazione di cui all'art. 1 del presente accordo - per esigenze di servizio rappresentate dal Dirigente Responsabile del Presidio e/o dal Dirigente del Responsabile del Servizio di appartenenza. Qualora impossibilitato al momento della richiesta, il dipendente è in ogni caso tenuto a presentarsi in sede entro le 24 ore successive.

8. Informativa

Il dipendente si impegna al rispetto di quanto previsto nell'Informativa sulla salute e sicurezza nel lavoro agile di cui, con la sottoscrizione del presente Accordo, conferma di averne preso visione e dichiara

□ di saper utilizzare i software gestionali in uso in ERAP, relativamente al proprio ambito lavorativo/settore di riferimento;

□ di conoscere le modalità operative del lavoro agile come approvate dal CdA con delibera n. ___/2023;

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

Data _____

Il Dipendente

Parere del Dirigente Responsabile del Servizio _____

Il Dirigente Responsabile del Presidio

PRESIDIO DI ANCONA
Piazza Salvo d'Acquisto n° 40 – 60131 Ancona
tel. (071) 28531 – fax (071) 2867028
mail: presidioan@erapmarche.it
pec: erap.marche.an@emarche.it

INFORMATIVA SULLA SALUTE E SICUREZZA NEL LAVORO AGILE AI SENSI DELL'ART. 22, COMMA 1, L. 81/2017

Al lavoratore

Oggetto: informativa sulla sicurezza dei lavoratori (art. 22, comma 1, della legge 22 maggio 2017 n. 81)

AVVERTENZE GENERALI

Si informano i dipendenti di ERAP MARCHE degli obblighi e dei diritti previsti dalla legge del 22 maggio 2017 n. 81 e dal decreto legislativo del 9 aprile 2008 n. 81.

Sicurezza sul lavoro (art. 22 L. 81/2017)

1. Il datore di lavoro garantisce la salute e la sicurezza del lavoratore, che svolge la prestazione in modalità di lavoro agile, e a tal fine consegna al lavoratore e al rappresentante dei lavoratori per la sicurezza, con cadenza almeno annuale, un'informativa scritta, nella quale sono individuati i rischi generali e i rischi specifici connessi alla particolare modalità di esecuzione del rapporto di lavoro.

2. Il lavoratore è tenuto a cooperare all'attuazione delle misure di prevenzione predisposte dal datore di lavoro per fronteggiare i rischi connessi all'esecuzione della prestazione all'esterno dei locali aziendali.

Obblighi dei lavoratori (art. 20 D. Lgs. 81/2008)

1. Ogni lavoratore deve prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro.

2. I lavoratori devono in particolare:

a) contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;

b) osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;

c) utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto, nonché i dispositivi di sicurezza;

d) utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;

e) segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi di cui alle lettere c) e d), nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;

f) non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;

PRESIDIO DI ANCONA
Piazza Salvo d'Acquisto n° 40 – 60131 Ancona
tel. (071) 28531 – fax (071) 2867028
mail: presidioan@erapmarche.it
pec: erap.marche.an@emarche.it

g) non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;

h) partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro;

i) sottoporsi ai controlli sanitari previsti dal D. Lgs. 81/2008 o comunque disposti dal medico competente.

3. I lavoratori di aziende che svolgono attività in regime di appalto o subappalto, devono esporre apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro. Tale obbligo grava anche in capo ai lavoratori autonomi che esercitano direttamente la propria attività nel medesimo luogo di lavoro, i quali sono tenuti a provvedervi per proprio conto.

In attuazione di quanto disposto dalla normativa in materia di salute e sicurezza sul lavoro, il Datore di Lavoro ha provveduto ad attuare le misure generali di tutela di cui all'art. 15 del T.U. sulla sicurezza; ha provveduto alla redazione del Documento di Valutazione di tutti i rischi presenti nella realtà lavorativa, ai sensi degli artt. 17 e 28 D. Lgs. 81/2008; ha provveduto alla formazione e informazione di tutti i lavoratori, ex artt. 36 e 37 del medesimo D. Lgs. 81/2008.

Pertanto, di seguito, si procede alla analitica informazione, con specifico riferimento alle modalità di lavoro per lo *smart worker*.

*** *** ***

COMPORTAMENTI DI PREVENZIONE GENERALE RICHIESTI ALLO *SMART WORKER*

- Cooperare con diligenza all'attuazione delle misure di prevenzione e protezione predisposte dal datore di lavoro (DL) per fronteggiare i rischi connessi all'esecuzione della prestazione in ambienti *indoor* e *outdoor* diversi da quelli di lavoro abituali.
- Non adottare condotte che possano generare rischi per la propria salute e sicurezza o per quella di terzi.
- Individuare, secondo le esigenze connesse alla prestazione stessa o dalla necessità del lavoratore di conciliare le esigenze di vita con quelle lavorative e adottando principi di ragionevolezza, i luoghi di lavoro per l'esecuzione della prestazione lavorativa in *smart working* rispettando le indicazioni previste dalla presente informativa.
- In ogni caso, evitare luoghi, ambienti, situazioni e circostanze da cui possa derivare un pericolo per la propria salute e sicurezza o per quella dei terzi.

Di seguito, le indicazioni che il lavoratore è tenuto ad osservare per prevenire i rischi per la salute e sicurezza legati allo svolgimento della prestazione in modalità di lavoro agile.

*** *** ***

erap Marche
ENTE REGIONALE PER L'ABITAZIONE PUBBLICA

PRESIDIO DI ANCONA
Piazza Salvo d'Acquisto n° 40 – 60131 Ancona
tel. (071) 28531 – fax (071) 2867028
mail: presidioan@erapmarche.it
pec: erap.marche.an@emarche.it

CAPITOLO 1

INDICAZIONI RELATIVE ALLO SVOLGIMENTO DI ATTIVITA' LAVORATIVA IN AMBIENTI *OUTDOOR*

Nello svolgere l'attività all'aperto si richiama il lavoratore ad adottare un comportamento coscienzioso e prudente, escludendo luoghi che lo esporrebbero a rischi aggiuntivi rispetto a quelli specifici della propria attività svolta in luoghi chiusi.

È opportuno non lavorare con dispositivi elettronici come *tablet* e *smartphone* o similari all'aperto, soprattutto se si nota una diminuzione di visibilità dei caratteri sullo schermo rispetto all'uso in locali al chiuso dovuta alla maggiore luminosità ambientale.

All'aperto inoltre aumenta il rischio di riflessi sullo schermo o di abbagliamento.

Pertanto le attività svolgibili all'aperto sono essenzialmente quelle di lettura di documenti cartacei o comunicazioni telefoniche o tramite servizi VOIP (ad es. Skype).

Fermo restando che va seguito il criterio di ragionevolezza nella scelta del luogo in cui svolgere la prestazione lavorativa, si raccomanda di:

- privilegiare luoghi ombreggiati per ridurre l'esposizione a radiazione solare ultravioletta (UV);
- evitare di esporsi a condizioni meteoclimatiche sfavorevoli quali caldo o freddo intenso;
- non frequentare aree con presenza di animali incustoditi o aree che non siano adeguatamente manutenute quali ad esempio aree verdi incolte, con degrado ambientale e/o con presenza di rifiuti;
- non svolgere l'attività in un luogo isolato in cui sia difficoltoso richiedere e ricevere soccorso;
- non svolgere l'attività in aree con presenza di sostanze combustibili e infiammabili (vedere capitolo 5);
- non svolgere l'attività in aree in cui non ci sia la possibilità di approvvigionarsi di acqua potabile;
- mettere in atto tutte le precauzioni che consuetamente si adottano svolgendo attività *outdoor* (ad es.: creme contro le punture, antistaminici, abbigliamento adeguato, quanto prescritto dal proprio medico per situazioni personali di maggiore sensibilità, intolleranza, allergia, ecc.), per quanto riguarda i potenziali pericoli da esposizione ad agenti biologici (ad es. morsi, graffi e punture di insetti o altri animali, esposizione ad allergeni pollinici, ecc.).

*** *** ***

CAPITOLO 2

INDICAZIONI RELATIVE AD AMBIENTI *INDOOR* PRIVATI

Di seguito vengono riportate le principali indicazioni relative ai requisiti igienico-sanitari previsti per i locali privati in cui possono operare i lavoratori destinati a svolgere il lavoro agile.

Raccomandazioni generali per i locali:

- le attività lavorative non possono essere svolte in locali tecnici o locali non abitabili (ad es. soffitte, seminterrati, rustici, box);
- adeguata disponibilità di servizi igienici e acqua potabile e presenza di impianti a norma (elettrico, termoidraulico, ecc.) adeguatamente manutenuti;

PRESIDIO DI ANCONA
Piazza Salvo d'Acquisto n° 40 – 60131 Ancona
tel. (071) 28531 – fax (071) 2867028
mail: presidioan@erapmarche.it
pec: erap.marche.an@emarche.it

- le superfici interne delle pareti non devono presentare tracce di condensazione permanente (muffe);
- i locali, eccettuati quelli destinati a servizi igienici, disimpegni, corridoi, vani-scala e ripostigli debbono fruire di illuminazione naturale diretta, adeguata alla destinazione d'uso e, a tale scopo, devono avere una superficie finestrata idonea;
- i locali devono essere muniti di impianti di illuminazione artificiale, generale e localizzata, atti a garantire un adeguato comfort visivo agli occupanti.

Indicazioni per l'illuminazione naturale ed artificiale:

- si raccomanda, soprattutto nei mesi estivi, di schermare le finestre (ad es. con tendaggi, appropriato utilizzo delle tapparelle, ecc.) allo scopo di evitare l'abbagliamento e limitare l'esposizione diretta alle radiazioni solari;
- l'illuminazione generale e specifica (lampade da tavolo) deve essere tale da garantire un illuminamento sufficiente e un contrasto appropriato tra lo schermo e l'ambiente circostante.
- è importante collocare le lampade in modo tale da evitare abbagliamenti diretti e/o riflessi e la proiezione di ombre che ostacolino il compito visivo mentre si svolge l'attività lavorativa.

Indicazioni per l'aerazione naturale ed artificiale:

- è opportuno garantire il ricambio dell'aria naturale o con ventilazione meccanica;
- evitare di esporsi a correnti d'aria fastidiose che colpiscano una zona circoscritta del corpo (ad es. la nuca, le gambe, ecc.);
- gli eventuali impianti di condizionamento dell'aria devono essere a norma e regolarmente manutenuti; i sistemi filtranti dell'impianto e i recipienti eventuali per la raccolta della condensa, vanno regolarmente ispezionati e puliti e, se necessario, sostituiti;
- evitare di regolare la temperatura a livelli troppo alti o troppo bassi (a seconda della stagione) rispetto alla temperatura esterna;
- evitare l'inalazione attiva e passiva del fumo di tabacco, soprattutto negli ambienti chiusi, in quanto molto pericolosa per la salute umana.

*** *** ***

CAPITOLO 3

UTILIZZO SICURO DI ATTREZZATURE/DISPOSITIVI DI LAVORO

Di seguito vengono riportate le principali indicazioni relative ai requisiti e al corretto utilizzo di attrezzature/dispositivi di lavoro, con specifico riferimento a quelle consegnate ai lavoratori destinati a svolgere il lavoro agile: *notebook*, *tablet* e *smartphone*.

Indicazioni generali:

- conservare in luoghi in cui siano facilmente reperibili e consultabili il manuale/istruzioni per l'uso redatte dal fabbricante;
- leggere il manuale/istruzioni per l'uso prima dell'utilizzo dei dispositivi, seguire le indicazioni del costruttore/importatore e tenere a mente le informazioni riguardanti i principi di sicurezza;

PRESIDIO DI ANCONA
Piazza Salvo d'Acquisto n° 40 – 60131 Ancona
tel. (071) 28531 – fax (071) 2867028
mail: presidioan@erapmarche.it
pec: erap.marche.an@emarche.it

- si raccomanda di utilizzare apparecchi elettrici integri, senza parti conduttrici in tensione accessibili (ad es. cavi di alimentazione con danni alla guaina isolante che rendano visibili i conduttori interni), e di interromperne immediatamente l'utilizzo in caso di emissione di scintille, fumo e/o odore di bruciato, provvedendo a spegnere l'apparecchio e disconnettere la spina dalla presa elettrica di alimentazione (se connesse);
- verificare periodicamente che le attrezzature siano integre e correttamente funzionanti, compresi i cavi elettrici e la spina di alimentazione;
- non collegare tra loro dispositivi o accessori incompatibili;
- effettuare la ricarica elettrica da prese di alimentazione integre e attraverso i dispositivi (cavi di collegamento, alimentatori) forniti in dotazione;
- disporre i cavi di alimentazione in modo da minimizzare il pericolo di inciampo;
- spegnere le attrezzature una volta terminati i lavori;
- controllare che tutte le attrezzature/dispositivi siano scollegate/i dall'impianto elettrico quando non utilizzati, specialmente per lunghi periodi;
- si raccomanda di collocare le attrezzature/dispositivi in modo da favorire la loro ventilazione e raffreddamento (non coperti e con le griglie di aerazione non ostruite) e di astenersi dall'uso nel caso di un loro anomalo riscaldamento;
- inserire le spine dei cavi di alimentazione delle attrezzature/dispositivi in prese compatibili (ad es. spine a poli allineati in prese a poli allineati, spine *schuko* in prese *schuko*). Utilizzare la presa solo se ben ancorata al muro e controllare che la spina sia completamente inserita nella presa a garanzia di un contatto certo ed ottimale;
- riporre le attrezzature in luogo sicuro, lontano da fonti di calore o di innesco, evitare di pigiare i cavi e di piegarli in corrispondenza delle giunzioni tra spina e cavo e tra cavo e connettore (la parte che serve per connettere l'attrezzatura al cavo di alimentazione);
- non effettuare operazioni di riparazione e manutenzione fai da te;
- lo schermo dei dispositivi è realizzato in vetro/cristallo e può rompersi in caso di caduta o a seguito di un forte urto. In caso di rottura dello schermo, evitare di toccare le schegge di vetro e non tentare di rimuovere il vetro rotto dal dispositivo; il dispositivo non dovrà essere usato fino a quando non sarà stato riparato;
- le batterie/accumulatori non vanno gettati nel fuoco (potrebbero esplodere), né smontati, tagliati, compressi, piegati, forati, danneggiati, manomessi, immersi o esposti all'acqua o altri liquidi;
- in caso di fuoriuscita di liquido dalle batterie/accumulatori, va evitato il contatto del liquido con la pelle o gli occhi; qualora si verificasse un contatto, la parte colpita va sciacquata immediatamente con abbondante acqua e va consultato un medico;
- segnalare tempestivamente al datore di lavoro eventuali malfunzionamenti, tenendo le attrezzature/dispositivi spenti e scollegati dall'impianto elettrico;
- è opportuno fare periodicamente delle brevi pause per distogliere la vista dallo schermo e sgranchirsi le gambe;
- è bene cambiare spesso posizione durante il lavoro anche sfruttando le caratteristiche di estrema maneggevolezza di *tablet* e *smartphone*, tenendo presente la possibilità di alternare la posizione eretta con quella seduta;

PRESIDIO DI ANCONA
Piazza Salvo d'Acquisto n° 40 – 60131 Ancona
tel. (071) 28531 – fax (071) 2867028
mail: presidioan@erapmarche.it
pec: erap.marche.an@emarche.it

- prima di iniziare a lavorare, orientare lo schermo verificando che la posizione rispetto alle fonti di luce naturale e artificiale sia tale da non creare riflessi fastidiosi (come ad es. nel caso in cui l'operatore sia posizionato con le spalle rivolte ad una finestra non adeguatamente schermata o sotto un punto luce a soffitto) o abbagliamenti (ad es. evitare di sedersi di fronte ad una finestra non adeguatamente schermata);
- in una situazione corretta lo schermo è posto perpendicolarmente rispetto alla finestra e ad una distanza tale da evitare riflessi e abbagliamenti;
- i *notebook, tablet* e *smartphone* hanno uno schermo con una superficie molto riflettente (schermi lucidi o *glossy*) per garantire una resa ottimale dei colori; tenere presente che l'utilizzo di tali schermi può causare affaticamento visivo e pertanto:
    - regolare la luminosità e il contrasto sullo schermo in modo ottimale;
    - durante la lettura, distogliere spesso lo sguardo dallo schermo per fissare oggetti lontani, così come si fa quando si lavora normalmente al computer fisso;
    - in tutti i casi in cui i caratteri sullo schermo del dispositivo mobile siano troppo piccoli, è importante ingrandire i caratteri a schermo e utilizzare la funzione zoom per non affaticare gli occhi;
    - non lavorare mai al buio.

Indicazioni per il lavoro con il *notebook*

In caso di attività che comportino la redazione o la revisione di lunghi testi, tabelle o simili è opportuno l'impiego del *notebook* con le seguenti raccomandazioni:

- sistemare il *notebook* su un idoneo supporto che consenta lo stabile posizionamento dell'attrezzatura e un comodo appoggio degli avambracci;
- il sedile di lavoro deve essere stabile e deve permettere una posizione comoda. In caso di lavoro prolungato, la seduta deve avere bordi smussati;
- è importante stare seduti con un comodo appoggio della zona lombare e su una seduta non rigida (eventualmente utilizzare dei cuscini poco spessi);
- durante il lavoro con il *notebook*, la schiena va mantenuta poggiata al sedile provvisto di supporto per la zona lombare, evitando di piegarla in avanti;
- mantenere gli avambracci, i polsi e le mani allineati durante l'uso della tastiera, evitando di piegare o angolare i polsi;
- è opportuno che gli avambracci siano appoggiati sul piano e non tenuti sospesi;
- utilizzare un piano di lavoro stabile, con una superficie a basso indice di riflessione, con altezza sufficiente per permettere l'alloggiamento e il movimento degli arti inferiori, in grado di consentire cambiamenti di posizione nonché l'ingresso del sedile e dei braccioli, se presenti, e permettere una disposizione comoda del dispositivo (*notebook*), dei documenti e del materiale accessorio;
- l'altezza del piano di lavoro e della seduta devono essere tali da consentire all'operatore in posizione seduta di avere gli angoli braccio/avambraccio e gamba/coscia ciascuno a circa 90°;
- la profondità del piano di lavoro deve essere tale da assicurare una adeguata distanza visiva dallo schermo;

PRESIDIO DI ANCONA
Piazza Salvo d'Acquisto n° 40 – 60131 Ancona
tel. (071) 28531 – fax (071) 2867028
mail: presidioan@erapmarche.it
pec: erap.marche.an@emarche.it

- in base alla statura, e se necessario per mantenere un angolo di 90° tra gamba e coscia, creare un poggiapiedi con un oggetto di dimensioni opportune.

In caso di uso su mezzi di trasporto (treni/aerei/ navi) in qualità di passeggeri o in locali pubblici:

- è possibile lavorare in un locale pubblico o in viaggio solo ove le condizioni siano sufficientemente confortevoli ed ergonomiche, prestando particolare attenzione alla comodità della seduta, all'appoggio lombare e alla posizione delle braccia rispetto al tavolino di appoggio;
- evitare lavori prolungati nel caso l'altezza della seduta sia troppo bassa o alta rispetto al piano di appoggio del *notebook*;
- osservare le disposizioni impartite dal personale viaggiante (autisti, controllori, personale di volo, ecc.);
- nelle imbarcazioni il *notebook* è utilizzabile solo nei casi in cui sia possibile predisporre una idonea postazione di lavoro al chiuso e in assenza di rollio/beccheggio della nave;
- se fosse necessario ricaricare, e se esistono prese elettriche per la ricarica dei dispositivi mobili a disposizione dei clienti, verificare che la presa non sia danneggiata e che sia normalmente ancorata al suo supporto parete;
- non utilizzare il *notebook* su autobus/tram, metropolitane, taxi e in macchina anche se si è passeggeri.

Indicazioni per il lavoro con *tablet* e *smartphone*

I *tablet* sono idonei prevalentemente alla gestione della posta elettronica e della documentazione, mentre gli *smartphone* sono idonei essenzialmente alla gestione della posta elettronica e alla lettura di brevi documenti.

In caso di impiego di *tablet* e *smartphone* si raccomanda di:

- effettuare frequenti pause, limitando il tempo di digitazione continuata;
- evitare di utilizzare questi dispositivi per scrivere lunghi testi;
- evitare di utilizzare tali attrezzature mentre si cammina, salvo che per rispondere a chiamate vocali prediligendo l'utilizzo dell'auricolare;
- per prevenire l'affaticamento visivo, evitare attività prolungate di lettura sullo *smartphone*;
- effettuare periodicamente esercizi di allungamento dei muscoli della mano e del pollice (*stretching*).

Indicazioni per l'utilizzo sicuro dello *smartphone* come telefono cellulare

- È bene utilizzare l'auricolare durante le chiamate, evitando di tenere il volume su livelli elevati;
- spegnere il dispositivo nelle aree in cui è vietato l'uso di telefoni cellulari/*smartphone* o quando può causare interferenze o situazioni di pericolo (in aereo, strutture sanitarie, luoghi a rischio di incendio/esplosione, ecc.);
- al fine di evitare potenziali interferenze con apparecchiature mediche impiantate seguire le indicazioni del medico competente e le specifiche indicazioni del produttore/importatore dell'apparecchiatura.

I dispositivi potrebbero interferire con gli apparecchi acustici. A tal fine:

- non tenere i dispositivi nel taschino;
- in caso di utilizzo posizionarli sull'orecchio opposto rispetto a quello su cui è installato l'apparecchio acustico;
- evitare di usare il dispositivo in caso di sospetta interferenza;
- un portatore di apparecchi acustici che usasse l'auricolare collegato al telefono/*smartphone* potrebbe avere difficoltà nell'udire i suoni dell'ambiente circostante. Non usare l'auricolare se questo può mettere a rischio la propria e l'altrui sicurezza.

PRESIDIO DI ANCONA
Piazza Salvo d'Acquisto n° 40 – 60131 Ancona
tel. (071) 28531 – fax (071) 2867028
mail: presidioan@erapmarche.it
pec: erap.marche.an@emarche.it

Nel caso in cui ci si trovi all'interno di un veicolo:

- non tenere mai in mano il telefono cellulare/*smartphone* durante la guida: le mani devono essere sempre tenute libere per poter condurre il veicolo;
- durante la guida usare il telefono cellulare/*smartphone* esclusivamente con l'auricolare o in modalità viva voce;
- inviare e leggere i messaggi solo durante le fermate in area di sosta o di servizio o se si viaggia in qualità di passeggeri;
- non tenere o trasportare liquidi infiammabili o materiali esplosivi in prossimità del dispositivo, dei suoi componenti o dei suoi accessori;
- non utilizzare il telefono cellulare/*smartphone* nelle aree di distribuzione di carburante;
- non collocare il dispositivo nell'area di espansione dell'airbag.

*** *** ***

CAPITOLO 4

INDICAZIONI RELATIVE A REQUISITI E CORRETTO UTILIZZO DI IMPIANTI ELETTRICI

Indicazioni relative ai requisiti e al corretto utilizzo di impianti elettrici, apparecchi/dispositivi elettrici utilizzatori, dispositivi di connessione elettrica temporanea.

Impianto elettrico

A. Requisiti:

1) i componenti dell'impianto elettrico utilizzato (prese, interruttori, ecc.) devono apparire privi di parti danneggiate;

2) le sue parti conduttrici in tensione non devono essere accessibili (ad es. a causa di scatole di derivazione prive di coperchio di chiusura o con coperchio danneggiato, di scatole per prese o interruttori prive di alcuni componenti, di canaline portacavi a vista prive di coperchi di chiusura o con coperchi danneggiati);

3) le parti dell'impianto devono risultare asciutte, pulite e non devono prodursi scintille, odori di bruciato e/o fumo;

4) nel caso di utilizzo della rete elettrica in locali privati, è necessario conoscere l'ubicazione del quadro elettrico e la funzione degli interruttori in esso contenuti per poter disconnettere la rete elettrica in caso di emergenza;

B. Indicazioni di corretto utilizzo:

- è buona norma che le zone antistanti i quadri elettrici, le prese e gli interruttori siano tenute sgombre e accessibili;
- evitare di accumulare o accostare materiali infiammabili (carta, stoffe, materiali sintetici di facile innesco, buste di plastica, ecc.) a ridosso dei componenti dell'impianto, e in particolare delle prese elettriche a parete, per evitare il rischio di incendio;
- è importante posizionare le lampade, specialmente quelle da tavolo, in modo tale che non vi sia contatto con materiali infiammabili.

Dispositivi di connessione elettrica temporanea

(prolunghe, adattatori, prese a ricettività multipla, avvolgicavo, ecc.).

A. Requisiti:

PRESIDIO DI ANCONA
Piazza Salvo d'Acquisto n° 40 – 60131 Ancona
tel. (071) 28531 – fax (071) 2867028
mail: presidioan@erapmarche.it
pec: erap.marche.an@emarche.it

- i dispositivi di connessione elettrica temporanea devono essere dotati di informazioni (targhetta) indicanti almeno la tensione nominale (ad es. 220-240 Volt), la corrente nominale (ad es. 10 Ampere) e la potenza massima ammissibile (ad es. 1500 Watt);
- i dispositivi di connessione elettrica temporanea che si intende utilizzare devono essere integri (la guaina del cavo, le prese e le spine non devono essere danneggiate), non avere parti conduttrici scoperte (a spina inserita), non devono emettere scintille, fumo e/o odore di bruciato durante il funzionamento.

B. Indicazioni di corretto utilizzo:

- l'utilizzo di dispositivi di connessione elettrica temporanea deve essere ridotto al minimo indispensabile e preferibilmente solo quando non siano disponibili punti di alimentazione più vicini e idonei;
- le prese e le spine degli apparecchi elettrici, dei dispositivi di connessione elettrica temporanea e dell'impianto elettrico devono essere compatibili tra loro (spine a poli allineati in prese a poli allineati,spine *schuko* in prese *schuko*) e, nel funzionamento, le spine devono essere inserite completamente nelle prese, in modo da evitare il danneggiamento delle prese e garantire un contatto certo;
- evitare di piegare, schiacciare, tirare prolunghe, spine, ecc.;
- disporre i cavi di alimentazione e/o le eventuali prolunghe con attenzione, in modo da minimizzare il pericolo di inciampo;
- verificare sempre che la potenza ammissibile dei dispositivi di connessione elettrica temporanea (ad es. presa multipla con 1500 Watt) sia maggiore della somma delle potenze assorbite dagli apparecchi elettrici collegati (ad es. PC 300 Watt + stampante 1000 Watt);
- fare attenzione a che i dispositivi di connessione elettrica temporanea non risultino particolarmente caldi durante il loro funzionamento;
- srotolare i cavi il più possibile o comunque disporli in modo tale da esporre la maggiore superficie libera per smaltire il calore prodotto durante il loro impiego.

CAPITOLO 5

INFORMATIVA RELATIVA AL RISCHIO INCENDI PER IL LAVORO "AGILE"

Indicazioni generali:

- identificare il luogo di lavoro (indirizzo esatto) e avere a disposizione i principali numeri telefonici dei soccorsi nazionali e locali (VVF, Polizia, ospedali, ecc.);
- prestare attenzione ad apparecchi di cottura e riscaldamento dotati di resistenza elettrica a vista o a fiamma libera (alimentati a combustibili solidi, liquidi o gassosi) in quanto possibili focolai di incendio e di rischio ustione. Inoltre, tenere presente che questi ultimi necessitano di adeguati ricambi d'aria per l'eliminazione dei gas combusti;
- rispettare il divieto di fumo laddove presente;
- non gettare mozziconi accesi nelle aree a verde all'esterno, nei vasi con piante e nei contenitori destinati ai rifiuti;
- non ostruire le vie di esodo e non bloccare la chiusura delle eventuali porte tagliafuoco.

Comportamento per principio di incendio:

- mantenere la calma;
- disattivare le utenze presenti (PC, termoconvettori, apparecchiature elettriche) staccandone anche le spine;
- avvertire i presenti all'interno dell'edificio o nelle zone circostanti *outdoor*, chiedere aiuto e, nel caso si valuti l'impossibilità di agire, chiamare i soccorsi telefonicamente (VVF, Polizia, ecc.), fornendo loro cognome, luogo dell'evento, situazione, affollamento, ecc.;
- se l'evento lo permette, in attesa o meno dell'arrivo di aiuto o dei soccorsi, provare a spegnere l'incendio attraverso i mezzi di estinzione presenti (acqua[1], coperte[2], estintori[3], ecc.);- non utilizzare acqua per estinguere l'incendio su apparecchiature o parti di impianto elettrico o quantomeno prima di avere disattivato la tensione dal quadro elettrico;
- se non si riesce ad estinguere l'incendio, abbandonare il luogo dell'evento (chiudendo le porte dietro di sé ma non a chiave) e aspettare all'esterno l'arrivo dei soccorsi per fornire indicazioni;
- se non è possibile abbandonare l'edificio, chiudersi all'interno di un'altra stanza tamponando la porta con panni umidi, se disponibili, per ostacolare la diffusione dei fumi all'interno, aprire la finestra e segnalare la propria presenza.

Nel caso si svolga lavoro agile in luogo pubblico o come ospiti in altro luogo di lavoro privato è importante:

- accertarsi dell'esistenza di divieti e limitazioni di esercizio imposti dalle strutture e rispettarli;
- prendere visione, soprattutto nel piano dove si è collocati, delle piantine particolareggiate a parete, della dislocazione dei mezzi antincendio, dei pulsanti di allarme, delle vie di esodo;
- visualizzare i numeri di emergenza interni che sono in genere riportati sulle piantine a parete (addetti lotta antincendio/emergenze/coordinatore per l'emergenza, ecc.);
- leggere attentamente le indicazioni scritte e quelle grafiche riportate in planimetria;
- rispettare il divieto di fumo;
- evitare di creare ingombri alla circolazione lungo le vie di esodo;
- segnalare al responsabile del luogo o ai lavoratori designati quali addetti ogni evento pericoloso, per persone e cose, rilevato nell'ambiente occupato.

---

[1] È idonea allo spegnimento di incendi di manufatti in legno o in stoffa ma non per incendi che originano dall'impianto o da attrezzature elettriche.

[2] In caso di principi di incendio dell'impianto elettrico o di altro tipo (purché si tratti di piccoli focolai) si possono utilizzare le coperte ignifughe o, in loro assenza, coperte di lana o di cotone spesso (evitare assolutamente materiali sintetici o di piume come i *pile* e i piumini) per soffocare il focolaio (si impedisce l'arrivo di ossigeno alla fiamma). Se particolarmente piccolo il focolaio può essere soffocato anche con un recipiente di metallo (ad es. un coperchio o una pentola di acciaio rovesciata).

[3] ESTINTORI A POLVERE (ABC)
Sono idonei per spegnere i fuochi generati da sostanze solide che formano brace (fuochi di classe A), da sostanze liquide (fuochi di classe B) e da sostanze gassose (fuochi di classe C). Gli estintori a polvere sono utilizzabili per lo spegnimento dei principi d'incendio di ogni sostanza anche in presenza d'impianti elettrici in tensione.
ESTINTORI AD ANIDRIDE CARBONICA (CO_2)
Sono idonei allo spegnimento di sostanze liquide (fuochi di classe B) e fuochi di sostanze gassose (fuochi di classe C); possono essere usati anche in presenza di impianti elettrici in tensione. Occorre prestare molta attenzione all'eccessivo raffreddamento che genera il gas: ustione da freddo alle persone e possibili rotture su elementi caldi (ad es.: motori o parti metalliche calde potrebbero rompersi per eccessivo raffreddamento superficiale). Non sono indicati per spegnere fuochi di classe A (sostanze solide che formano brace). A causa dell'elevata pressione interna l'estintore a CO_2 risulta molto più pesante degli altri estintori a pari quantità di estinguente.
ISTRUZIONI PER L'UTILIZZO DELL'ESTINTORE
- sganciare l'estintore dall'eventuale supporto e porlo a terra;
- rompere il sigillo ed estrarre la spinetta di sicurezza;
- impugnare il tubo erogatore o manichetta;
- con l'altra mano, impugnata la maniglia dell'estintore, premere la valvola di apertura;
- dirigere il getto alla base delle fiamme premendo la leva prima ad intermittenza e poi con maggiore progressione;
- iniziare lo spegnimento delle fiamme più vicine a sé e solo dopo verso il focolaio principale.

PRESIDIO DI ANCONA
Piazza Salvo d'Acquisto n° 40 – 60131 Ancona
tel. (071) 28531 – fax (071) 2867028
mail: presidioan@erapmarche.it
pec: erap.marche.an@emarche.it

*** *** ***

- Di seguito si riporta una tabella riepilogativa al fine di indicare in quali dei diversi scenari lavorativi dovranno trovare applicazione le informazioni contenute nei cinque capitoli di cui sopra

Scenario lavorativo	**Attrezzatura utilizzabile**	**Capitoli da applicare**				
		1	**2**	**3**	**4**	**5**
1. Lavoro agile in locali privati al chiuso	Smartphone Auricolare Tablet Notebook		**X**	**X**	**X**	**X**
2. Lavoro agile in locali pubblici al chiuso	Smartphone Auricolare Tablet Notebook			**X**	**X**	**X**
3. Lavoro agile nei trasferimenti, su mezzi privati come passeggero o su autobus/tram, metropolitane e taxi	Smartphone Auricolare			**X**		
4. Lavoro agile nei trasferimenti su mezzi sui quali sia assicurato il posto a sedere e con tavolino di appoggio quali aerei, treni, autolinee extraurbane, imbarcazioni (traghetti e similari)	Smartphone Auricolare Tablet Notebook			**X**	**X**	
5. Lavoro agile nei luoghi all'aperto	Smartphone Auricolare Tablet Notebook	**X**		**X**		**X**

Allegato 2

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

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

REV.	DATA	DESCRIZIONE	APPROV.
1.0	23/11/2023	Prima emissione	

NOTE REVISIONE / EDIZIONE / APPLICAZIONE

Sommario

1 Introduzione

L'ERAP Marche nell'espletamento della sua attività istituzionale opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

Il presente documento definisce le regole e le condizioni per l'utilizzo degli **strumenti informatici dell'ERAP Marche** da parte dei dipendenti e di tutti coloro che, in virtù di un rapporto di lavoro a qualsiasi titolo (collaboratori, consulenti, stagisti, fornitori, etc.), utilizzano strumenti informatici dell'Agenzia, nel seguito denominati Utenti.

Il presente disciplinare deve considerarsi integrato da tutte le procedure interne adottate in ERAP Marche, fra cui la procedura prevista in caso di violazione di dati personali.

1.1 Finalità del documento

Il presente documento definisce e detta agli Utenti specifiche regole e condizioni di utilizzo degli strumenti informatici aziendali attraverso:

- definizione di regole e procedure uniformi da applicarsi in tutte le aree operative;
- indicazione delle principali disposizioni normative in materia di utilizzo dei sistemi informativi e di protezione dei dati personali;
- definizione dell'ambito, delle modalità e dei limiti del monitoraggio e dei controlli attuabili dell'ERAP Marche nel rispetto della normativa vigente nonché delle regole e delle procedure interne;
- individuazione delle responsabilità degli Utenti in caso di inosservanza di regole e prescrizioni.

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

Il presente documento integra e aggiorna quanto previsto nel "Regolamento interno relativo alla tutela dei dati personali trattati dell'Ente Regionale per l'Abitazione Pubblica delle Marche" approvato con delibera del CDA n. 171 del 18/11/2029 che qui si richiama integralmente;

1.2 Contesto normativo

Il presente disciplinare è redatto sulla base dei seguenti e principali riferimenti normativi:

- Codice penale, con particolare riferimento ai reati informatici;
- L. 300/1970 (Statuto dei lavoratori) - artt. 4, 7 e 8;
- D. Lgs. 196/2003 e s.m.i (Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per posta elettronica e Internet" di cui alla deliberazione 13/2007;
- D. Lgs. 81/2008 e s.m.i (Testo Unico sulla sicurezza);
- D.P.R 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione) e Codice di comportamento AgID;
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR)
- Regolamento interno relativo alla tutela dei dati personali trattati dell'Ente Regionale per l'Abitazione Pubblica delle Marche (di seguito **Reg. Privacy**);

1.3 Definizioni

Termini	Definizione
AdS	Amministratore di Sistema, figure professionali finalizzate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009;
Applicazioni aziendali	si considerano applicazioni aziendali: • Prodotti/programmi acquistati dall'amministrazione, di valenza generale o settoriale ed in quest'ultimo caso approvati dal Settore Informatica e Digitalizzazione; • Applicazioni e servizio sviluppate ad hoc dal Settore Informatica e Digitalizzazione, da terze parti ma sotto il coordinamento del Settore Informatica e Digitalizzazione ovvero da altre strutture con un processo di partecipazione e approvazione da parte del Settore Informatica e Digitalizzazione e che seguono le regole di gestione previste nei casi precedenti; • Applicazioni esterne che l'amministrazione utilizza secondo le regole di gestione e di sicurezza delle medesime a titolo di mero esempio possono essere la piattaforma NoiPA, abbonamenti a servizi informativi, portale ANAC, etc.
Backup	Salvataggio periodico e programmato dei dati

Collaboratori	Personale dipendente, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni e coloro che, in virtù di un rapporto di lavoro in essere a qualsiasi titolo con l'ERAP Marche, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione dall'ERAP.
Disaster recovery	Ripristino del sistema e dei dati a seguito di un evento distruttivo
Dispositivi mobili	apparecchi di telecomunicazione portatili (tablet, smartphone, etc.);
File di log	registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato;
Freeware	Software distribuito gratuitamente e senza bisogno di licenza d'uso, per lo più reperibile attraverso Internet.
Guest book	Libro degli ospiti inteso in informatica come un sito dove poter lasciare i propri dati per esprimere un giudizio o commento
Host	Computer o server sul quale sono memorizzate le informazioni cui altri strumenti informatici (detti client) possono accedere per mezzo di un collegamento telematico. In partic. si chiama h. il computer che ospita un sito web accessibile via Internet.
ICT	Information & Communication Technology – Tecnologie Informatiche e di Comunicazione
LOG	Vedi File di log
Nick name	Nominativo (o soprannome) utilizzato tipicamente per la registrazione utente su servizi on-line
Pila software	elenco di software installati o installabili sui dispositivi aziendali di ERAP Marche;
Postazioni di lavoro (PdL)	personal computer (desktop o portatile) messo a disposizione da ERAP Marche a ciascun Collaboratore per l'espletamento dell'attività lavorativa;
Shareware	Software che può essere provato gratuitamente, pur rimanendo vincolato al diritto d'autore
Sistema informativo interno	si intende sia la rete interna, sia ogni strumento informatico ad esso collegato (pc, tablet, telefoni…)
Strumenti informatici	personal computer fissi o portatili, stampanti locali o di rete, programmi e prodotti software, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc);
VPN	Virtual Private Network (Rete virtuale privata); permette di creare una connessione di rete privata tra dispositivi su Internet. Le VPN sono utilizzate per trasmettere dati sulle reti pubbliche in modo anonimo e sicuro; nello specifico ERAP Marche utilizza questa tecnologia per creare un collegamento sicuro tra uno strumento informatico collegato ad internet e la rete interna dell'Ente.

1.4 Ambito di applicazione

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

2 Linee guida e misure tecniche ed organizzative

2.1 Figure e ruoli all'interno della Organizzazione di ERAP Marche in ambito di sicurezza informatica

La gestione della sicurezza informatica costituisce parte essenziale delle misure e delle attività da mettere in atto anche nell'ambito della tutela dei dati personali. Pertanto, è qui richiamato l'art. 3 del Reg. Privacy che individua la gerarchia di responsabilità e l'esercizio delle funzioni di titolare del trattamento dei dati personali. Di conseguenza, sono individuate le seguenti figure interne all'organizzazione di ERAP Marche alle quali sono affidati compiti e funzioni in materia di sicurezza informatica:

- Il Presidente del consiglio di amministrazione;
- Il segretario del consiglio di amministrazione (di seguito Segretario)
- I Responsabili dei presidi;
- I Dirigenti;
- Responsabili di settore e/o posizione organizzativa.

Si occupano inoltre specificatamente di sicurezza informatica le seguenti figure:

- Responsabile del settore Informatica e Digitalizzazione
- Referenti informatici di Struttura
- Amministratori di sistema (AdS)
- Responsabile della protezione dei dati (DPO)

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

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

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

2.2 Strumenti informatici

Gli strumenti informatici sono assegnati agli Utenti per lo svolgimento dell'attività lavorativa e devono essere utilizzati con modalità e mediante comportamenti adeguati ai compiti assegnati e alle responsabilità connesse, nel rispetto del Codice di comportamento dei dipendenti della pubblica amministrazione e delle normative e direttive interne.

Nell'esecuzione della propria attività lavorativa, gli Utenti sono tenuti ad attenersi alle seguenti istruzioni generali:

a) effettuare la propria attività uniformandosi alle disposizioni dell'ERAP Marche e alle istruzioni ricevute;
b) custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente alle strutture preposte, secondo le modalità previste, ogni danneggiamento, smarrimento o furto;
c) mantenere la riservatezza sulle informazioni e sui dati personali di cui siano venuti a conoscenza durante lo svolgimento della propria attività;
d) in caso di cessazione dal servizio o dalla prestazione svolta per ERAP Marche, astenersi dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività;
e) adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati;
f) garantire la corretta custodia di atti e documenti adottati da ERAP Marche.

Si richiama quando disciplinato agli artt. 19 e ss. Del Reg. Privacy.

2.3 Disciplina dell'accesso alle risorse informatiche di ERAP Marche

2.3.1 Regole di accesso alla rete informatica

L'accesso alle applicazioni del sistema informativo dell'ERAP Marche avviene attraverso autenticazione mediante credenziali di dominio.

Le credenziali di autenticazione, da gestire nel rispetto delle regole stabilite, sono strettamente personali e non devono essere comunicate né rese disponibili ad altri soggetti.

In caso di diffusione accidentale, anche solo presunta, le password devono essere immediatamente modificate e l'incidente va immediatamente segnalato.

Il sistema di controllo degli accessi presente in ERAP Marche implementa le seguenti regole:

- composizione di password complesse, che abbiano una lunghezza minima stabilita e una sequenza di caratteri normali, speciali e/o numerici;
- modifica della password al primo utilizzo;
- validità minima e massima della password;
- impossibilità di riuso delle ultime password utilizzate;
- blocco dell'utenza dopo un determinato numero di tentativi falliti di inserimento della password;
- reinizializzazione (reset) della password e riattivazione delle utenze disabilitate, secondo le procedure in vigore.

I dettagli dei requisiti richiesti sull'utilizzo delle password sono riportati all'art. 22 del Reg.Privacy.

Il Collaboratore è tenuto a sostituire la propria password ogni volta che sospetta che la stessa non sia più segreta. La password deve essere cambiata almeno una volta ogni 90 giorni.

Nel caso in cui, per motivi tecnici od organizzativi, non sia possibile cambiare in autonomia la password ai sistemi, è responsabilità di ogni collaboratore richiedere l'intervento Settore Informatica e Digitalizzazione.

Qualora il Collaboratore venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Dirigente di riferimento (o persona da questa incaricata) o alil Settore Informatica e Digialization, oppure al custode delle password, ove previsto.

Al fine di aumentare il livello di sicurezza, ERAP Marche ha scelto di implementare un sistema do autenticazione multi-fattore o Multi Factor Authentication (MFA), richiedendo all'Utente di dimostrare la propria identità attraverso più forme di verifica al momento dell'accesso a un'applicazione una delle quali prevede l'utilizzo dello smartphone in possesso dell'utente.

Attualmente sono disponibili tre modalità:

- Il sistema invia un codice numerico (OTP) tramite messaggio di testo (SMS);
- Il sistema invia un codice numerico (OTP) tramite chiamata telefonica vocale;

- Tramite App mobile Microsoft Authenticator gli accessi vengono approvati, a scelta del dipendente, mediante notifiche push, biometrie o passcode monouso. Si evidenzia che, nell'ipotesi di utilizzo del dato biometrico costituito dall'impronta digitale, questo non è trattato da ERAP Marche ma resta salvato nella memoria del dispositivo utilizzato ed è cancellato al momento dell'eventuale riconsegna del dispositivo da parte dell'Utente.

2.3.2 Regole di accesso alla rete fisica

Tutte le postazioni di lavoro collegate alla rete fisica dell'ERAP Marche devono utilizzare un insieme di servizi di rete (Microsoft Active Directory su dominio "eraprm.local") per garantire il rispetto di criteri di gruppo, una gestione delle autenticazione alla rete aziendale centralizzata e la distribuzione automatica degli aggiornamenti, delle politiche di sicurezza e dei software antivirus ed antimalware.
La policy di accesso al dominio prevede l'attivazione automatica della complessità della password e della scadenza forzata ogni 90 giorni.
Se il Dirigente autorizza un collaboratore all'accesso alle risorse di dominio di ERAP Marche (caselle di posta, cartelle condivise di rete, accesso a banche dati o applicativi ecc.) lo fa sotto la propria responsabilità vigilando costantemente l'operato dell'utente, impartendo apposite istruzioni e vincoli contrattuali che garantiscano l'applicazione delle misure di sicurezza tecniche e organizzative, la riservatezza delle informazioni e dei dati che tratteranno e la divulgazione non autorizzata.

2.3.3 Accesso da remoto al sistema ICT di ERAP Marche

Per accedere alle risorse informatiche di ERAP Marche dall'esterno, è necessario autenticarsi utilizzando il sistema di autenticazione multi-fattore messo a disposizione di ERAP Marche descritto al punto 2.3.1.
Questo sistema aumenta la sicurezza informatica di ERAP Marche impedendo l'accesso ai male intenzionati che siano riusciti ad individuare le credenziali di accesso dell'utente.
Gli utenti che devono accedere sono autorizzati, nel caso in cui non dispongano di uno smartphone di servizio, ad utilizzare il loro smartphone personale.
L'utente è tenuto a custodire lo smartphone e i metodi di autenticazione utilizzati con la massima cura ed è tenuto ad avvisare immediatamente il Settore Informatica e Digitalizzazione in caso di smarrimento o presunta compromissione della sicurezza dell'apparato.

2.3.4 Regole di disattivazione

Richiamando e integrando quanto disciplinato all'art.31 del Reg. Privacy, si dispone quanto segue.
Le credenziali di autenticazione non utilizzate da almeno tre mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica, organizzativa o di servizio; anche in questo caso il Settore Informatica e Digitalizzazione si fa garante della gestione degli account tecnici utilizzati.

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

La cessazione degli utenti di dominio dovrà avvenire in maniera puntuale: in caso di cessazione del rapporto di collaborazione/consulenza, il Dirigente è obbligato ad avvisare immediatamente il Settore Informatica e Digitalizzazione per l'immediata disattivazione dell'utente.

Il Dirigente deve porre la massima attenzione al caso in cui sia necessario modificare le autorizzazioni precedentemente assegnate all'utente per accedere alle risorse di dominio quali caselle di posta generiche/ufficiali, cartelle condivise, banche dati o applicativi, ad esempio quando ciò sia necessario, o per effetto di una riorganizzazione o per lo spostamento di dipendenti tra gli uffici o i Presidi, o per cambio di mansioni; in questo caso, il Dirigente deve prontamente comunicare al settore Informatica e Digitalizzazione i cambi da effettuare, utilizzando le procedure messe a disposizione per questo scopo o, in mancanza, tramite una comunicazione via posta elettronica.

All'atto della cessazione/interruzione del rapporto di lavoro o dell'attività lavorativa svolta a qualsiasi titolo per conto dell'ERAP Marche, ferma restando la disabilitazione all'uso degli applicativi e delle funzionalità di ERAP Marche da parte del Settore Informatica e Digitalizzazione, è fatto obbligo di restituzione delle strumentazioni elettroniche (pc portatili, tablet, cellulari, kit di firma elettronica ecc.) già affidate per l'esplicazione delle funzioni connesse al rapporto di lavoro.

In caso di assegnazione temporanea del personale ERAP Marche presso altra pubblica amministrazione, la titolarità della casella di posta elettronica sul dominio dell'ERAP Marche potrà essere mantenuta nel rispetto delle disposizioni che regolano l'uso di tale risorsa ai sensi del presente disciplinare. All'atto dell'assegnazione temporanea e durante il relativo periodo di servizio, il Settore Informatica e Digitalizzazione provvede alla disabilitazione all'uso degli applicativi e funzionalità, fermo restando l'obbligo del dipendente di restituzione della strumentazione informatica già assegnata dall'ERAP Marche per lo svolgimento della prestazione lavorativa.

2.4 Postazioni di lavoro

Ad integrazione di quanto già disciplinato negli art. 16 e ss. Del Reg. Privacy, qui richiamati integralmente, si dispone quanto segue.

Le postazioni di lavoro (PdL) sono gestite dal Settore Informatica e Digitalizzazione che le assegna ai Collaboratori. È vietato qualsiasi utilizzo che deturpi o rovini la PdL e tutti gli accessori/periferiche in assegnazione.

La postazione di lavoro è provvista di software di sicurezza (software antivirus, personal firewall, software per aggiornamento automatico delle patch di sistema, etc.).

L'assegnatario della PdL è profilato come utente senza diritti amministrativi.

La PdL è provvista del software base approvato dall'ERAP Marche. In caso di particolari necessità, è disponibile una lista di software, la cui installazione può essere richiesta direttamente dall'Utente al Settore Informatica e Digitalizzazione tramite l'Helpdesk. Ulteriori necessità lavorative potranno essere rappresentate al Settore Informatica e Digitalizzazione, che valuterà l'ammissibilità delle richieste.

Il Collaboratore assegnatario della postazione di lavoro è responsabile del suo corretto utilizzo nel rispetto delle seguenti regole comportamentali:

a) la PdL è assegnata al Collaboratore per lo svolgimento della propria attività lavorativa; è consentito l'uso promiscuo, sia lavorativo sia personale, delle PdL;
b) la PdL non deve essere accessibile a soggetti non autorizzati;
c) il Collaboratore non deve apportare modifiche alle configurazioni della PdL che non siano state preventivamente richieste e autorizzate dal Settore Informatica e Digitalizzazione;
d) tutto il personale ha l'obbligo di salvare la documentazione relativa alla propria attività lavorativa sugli spazi di condivisione aziendali;
e) durante l'allontanamento dalla PdL, il Collaboratore deve bloccare la propria postazione per consentirne l'accesso unicamente mediante l'immissione della password;
f) al termine della giornata lavorativa, soprattutto per motivi di sicurezza, e salvo che il Collaboratore preveda di dover utilizzare la PdL da remoto, deve essere effettuato lo spegnimento delle PdL.

2.4.1 Postazione di lavoro portatile

Per quanto riguarda la postazione portatile, valgono tutte le regole già descritte per le postazioni fisse. Si evidenzia che le stazioni di lavoro portatili, utilizzate al di fuori dell'ERAP Marche, sono maggiormente esposte a rischi di sicurezza, quali danneggiamenti conseguenti agli spostamenti, furti, violazione della riservatezza delle informazioni contenute. Tutti i Collaboratori, pertanto, devono custodire con cura e diligenza la postazione di lavoro portatile assegnata.

Le postazioni di lavoro portatili devono essere verificate dal Settore Informatica e Digitalizzazione per l'installazione di eventuali aggiornamenti e/o patch di sicurezza. La verifica avviene mediante appuntamento concordato con il Settore stesso. In caso di significativo rischio di compromissione o/e sicurezza, tale Settore può richiedere al Collaboratore lo spegnimento della PdL portatile fino a tale verifica ovvero bloccare il dispositivo da remoto.

2.4.2 Altri dispositivi

Con riferimento ad altri dispositivi assegnati ai dipendenti, quali smartphone e/o tablet, valgono le medesime regole comportamentali adottate per le PdL.

2.5 Software a corredo

All'interno dell'organizzazione, in merito all'installazione/utilizzo dei software, il Settore Informatica e Digitalizzazione ha la responsabilità di:

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

Alla luce della già menzionata responsabilità esclusiva del Settore Informatica e Digitalizzazione, è vietato l'utilizzo/installazione di qualsiasi software/applicazione non precedentemente autorizzato dalla struttura stessa.

La lista software autorizzato dal Settore Informatica e Digitalizzazione è contenuta nel documento denominato Pila Software (disponibile nel gruppo Microsoft Teams ERAP Marche – canale Privacy e sicurezza informatica) e riguarda tutti i dispositivi aziendali.

Con un apposito modulo che sarà disponibile online o altre modalità telematiche che saranno comunicate, il dirigente dovrà richiedere l'autorizzazione di installazione per software necessari ai fini lavorativi.

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

L'eventuale utilizzo di software di tipo portable (che non richiedono installazione) o installabili con i permessi dell'Utente è nella completa responsabilità dell'Utente, sia per gli aspetti di diritto di proprietà intellettuale sia per quelli di sicurezza.

Non è permessa l'installazione di software aziendale con licenza ERAP Marche su dispositivi privati.

2.6 Navigazione in internet

Ad integrazione di quanto già disciplinato nell'art. 24 Del Reg. Privacy, qui richiamato integralmente, si dispone quanto segue.

La navigazione in internet è messa a disposizione del personale come fonte di informazione per le finalità di documentazione, ricerca e studio, utili per lo svolgimento della prestazione lavorativa.

Qualsiasi operazione effettuata sulla rete esterna (accesso a siti web per necessità non inerenti all'attività lavorativa, salvataggio di file, partecipazione a forum, etc.) è posta sotto la responsabilità del Collaboratore, che deve mantenere un comportamento lecito e tale da non compromettere le attività e il buon nome dell'ERAP Marche.

Ogni Collaboratore è tenuto a osservare le seguenti regole comportamentali:

- utilizzare internet per fini leciti, astenendosi da qualsiasi comportamento che possa avere natura oltraggiosa e/o discriminatoria verso terzi;
- trasferire sul proprio computer (download) solo file da siti web verificati e affidabili, tenendo presente che quando si trasferisce materiale da internet occorre prestare la massima attenzione al fine di non incorrere in violazioni di diritti di proprietà intellettuale;
- non utilizzare social network, forum, chat e simili per scambiare informazioni riservate o lesive dell'immagine dell'ERAP Marche e dei colleghi;
- la navigazione in internet avviene in modalità trasparente e non anonima, soprattutto se attraverso intranet o strumenti aziendali; in ogni caso è vietato accedere a siti i cui contenuti non siano adeguati all'immagine e al buon nome dell'Agenzia.

Al fine di prevenire l'accesso a siti web e risorse internet potenzialmente nocivi, per la navigazione dalla rete aziendale l'ERAP Marche adotta soluzioni di sicurezza basate su filtri e decriptazione delle informazioni della navigazione Internet (ad esclusione di determinate categorie di siti individuati da ERAP Marche, ad esempio siti bancari, sanitari, ecc.) attraverso i quali l'accesso a specifiche e determinate categorie di siti è bloccato a priori; i tentativi di accesso a tali siti (ad esempio siti malevoli, gioco d'azzardo, siti per adulti) vengono bloccati e al Collaboratore è inviato un avviso in cui viene spiegato il motivo del blocco. (si veda l'appendice A al Reg. Privacy per quanto riguarda la tipologia di siti filtrati).

Al fine di prevenire il download di file o pagine web contenenti codici malevoli, l'ERAP Marche adotta soluzioni di sicurezza basate su tecnologie antimalware che effettuano la scansione dei contenuti della navigazione Internet e bloccano il download del contenuto in caso di rilevazione di codice malevolo.

Si rinvia all'

2.7 Posta elettronica

Ad integrazione di quanto già disciplinato nell'art. 23 Del Reg. Privacy, qui richiamato integralmente, si dispone quanto segue.

Tutti gli Utenti sono dotati di una casella di posta elettronica sul dominio dell'ERAP Marche. Le caselle devono essere utilizzate per l'esercizio della propria attività lavorativa.

L'utilizzo delle caselle PEC gestite in ambito generale o funzionale ad applicazioni dal personale che ne cura le relative applicazioni è coordinato dal dirigente di riferimento. Laddove vi fosse la necessità di istituire caselle PEC nominali queste devono essere utilizzate esclusivamente per motivi di ufficio in conformità alle regole del presente disciplinare e alle disposizioni impartite dal dirigente responsabile.

Il sistema di posta elettronica prevede:

- la possibilità di imporre limiti all'utilizzo del servizio, ad esempio sul numero dei destinatari di un messaggio, sulla dimensione degli allegati che sarà possibile inviare e/o sulla dimensione complessiva della casella di posta elettronica. L'utilizzo degli indirizzi di posta elettronica interna collettivi di ERAP Marche (ad esempio tutticolleghierap@erapmarche.it) è riservato alla Presidenza, ai Responsabili di Presidio e ai soggetti che svolgono attività di comunicazione e informazione connesse allo svolgimento delle funzioni istituzionali di competenza. L'invio di comunicazioni agli indirizzi di posta elettronica interna collettivi è altresì consentito alle organizzazioni sindacali aventi titolo, tramite la casella di posta elettronica abilitata, esclusivamente per lo svolgimento delle attività di competenza nell'esercizio dell'attività sindacale. Gli indirizzi di posta elettronica interna collettivi restano comunque aperti e potranno essere eccezionalmente utilizzati in casi particolari, previa autorizzazione del proprio dirigente, nel rispetto del principio di responsabilità del Collaboratore ed evitando di ingenerare risposte multiple attraverso l'utilizzo della funzione di reply all.
- per le e-mail inviate a destinatari esterni al dominio di posta elettronica dell'Agenzia, è predisposto un avvertimento (disclaimer) inserito automaticamente in calce al messaggio. In tale disclaimer viene dichiarata la natura riservata del contenuto ed è inserito un invito alla cancellazione per chi non fosse il destinatario previsto. Non è consentito inserire disclaimer personalizzati in calce alla comunicazione;
- una scansione di sicurezza dei messaggi mediante strumenti automatici, al fine di prevenire la diffusione di e-mail contenenti malware e/o phishing; a fronte di tale controllo si potrebbe rendere necessario l'accesso, da parte dell'Amministratore di Sistema, ai singoli messaggi identificati come potenzialmente malevoli;
- un sistema automatico di classificazione dei messaggi ricevuti (spam o posta indesiderata), in cui confluiscono tutti i messaggi non reputati leciti dall'algoritmo anti-spamming.

Nell'utilizzo del servizio il Collaboratore ha l'obbligo di:

- proteggere la privacy dell'interlocutore evitando, qualora non necessario, di inoltrare messaggi altrui senza il previo consenso dell'interessato;
- inviare le e-mail esclusivamente a nome proprio. Si ricorda che è considerato mittente il proprietario della casella da cui è inviata l'e-mail, anche in presenza di altri nominativi;
- evitare l'invio, tramite le caselle di posta elettronica, di messaggi ingiuriosi, minatori, lesivi dell'immagine dell'Agenzia o che utilizzino linguaggi o immagini oscene, ingannevoli o diffamatorie;
- evitare di creare o rispondere a "catene di Sant'Antonio", appelli o richieste non pertinenti all'attività lavorativa in ERAP Marche;
- evitare l'invio o l'inoltro di messaggi estranei al contesto lavorativo a un gran numero di indirizzi o a liste di distribuzione interne all'ERAP Marche;

- evitare l'utilizzo dell'indirizzo e-mail per l'iscrizione e/o la partecipazione a social network, mailing list, servizi di instant messaging, forum o altri servizi pubblici su internet di interesse personale e non lavorativo;
- evitare di diffondere, all'esterno dell'ERAP Marche, indirizzi di posta elettronica di altri colleghi, per motivi non legati all'attività lavorativa.

L'ERAP Marche ha definito specifiche modalità per assicurare la disponibilità di informazioni in caso di assenza improvvisa o prolungata di un Collaboratore. Fermo restando che i contenuti delle e-mail sono ordinariamente consultabili esclusivamente da parte del Collaboratore titolare della casella, vengono adottate le seguenti misure di tipo tecnologico:

- possibilità di attivazione da parte del Collaboratore, in caso di sua assenza prolungata, della funzione di risposta automatica con invito al mittente a prendere contatto con l'Ufficio competente dell'ERAP Marche.

Quando si utilizza lo strumento della posta elettronica, è opportuno osservare comportamenti consoni, ed in particolare:

- Assicurarsi di aver letto accuratamente e compreso il messaggio a cui si risponde.
- Rispondere solo a chi ci ha scritto, coinvolgendo terzi unicamente se necessario o se funzionale all'efficienza dell'ufficio.
- Assicurarsi dei corretti destinatari della comunicazione, onde evitare di coinvolgere persone non interessate.
- Specificare sempre, nel campo "oggetto", l'argomento del proprio messaggio in modo chiaro, sintetico e inequivocabile.
- Scrivere in modo chiaro e sintetico.
- Inserire allegati solo se non disponibili in spazi di condivisione aziendale o reperibili in rete.
- Chiedere al destinatario la conferma di lettura unicamente se necessario.
- Rileggere e controllare il proprio messaggio prima di inviarlo, per:
  - evitare errori materiali che possano dare un'impressione di scarsa accuratezza;
  - smussare asperità o toni che possano risultare irritanti o offensivi (ad es.: scrivere TUTTO MAIUSCOLO equivale a gridare);
  - essere certi dell'univocità dei contenuti, per non essere fraintesi.

Fermo restando le tutele e le garanzie a livello costituzionale, in ambito civile e penale e dalla normativa in materia di protezione dei dati, nei casi previsti dall'art. 23 del Reg. Privacy, l'ERAP Marche può accedere alle informazioni ivi contenute, alle seguenti condizioni:

- il Collaboratore deve essere preventivamente avvisato, con modalità idonea a garantirne l'effettiva informazione, della facoltà dell'ERAP Marche di accedere alla sua casella e-mail e alla relativa corrispondenza;
- il controllo delle e-mail non può superare i limiti imposti dalla finalità del trattamento, ragione

per cui il controllo deve essere limitato alla corrispondenza attinenti alle questioni che coinvolgono l'amministrazione e che hanno reso necessario l'intervento;

- l'Amministrazione deve consentire la "tracciabilità dei controlli", in modo da rendere chiaro quanti e quali messaggi sono stati monitorati, per quanto tempo e quante persone hanno avuto accesso ai risultati della sorveglianza;
- deve essere rispettato il principio di proporzionalità tra finalità perseguita e tutela della riservatezza, per cui non sono consentiti controlli massivi, attivati in assenza di un motivo specifico o di un pericolo attuale.
- nel caso di fondato sospetto di infedeltà del Collaboratore, al fine della ricerca di elementi oggettivi comprovanti la stessa.

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

Decorsi due mesi, l'account verrà disabilitato, disattivando anche il messaggio di risposta automatica. L'ERAP Marche potrà accedere ai contenuti della casella di posta disattivata per un periodo massimo di 3 mesi.

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

Tutte le disposizioni relative alle caselle di posta elettronica interna assegnata al Collaboratore devono ritenersi valide, per quanto compatibili, anche per qualsiasi altro strumento di messaggistica o corrispondenza elettronica messo a disposizione dell'ERAP Marche ai Collaboratori.

2.8 Servizi di Unified Communication (chat, messaggistica, videoconferenza, telefonia)

Gli strumenti di Unified Communication (UC), oltre alla posta elettronica, comprendono la chat, la telefonia, la videoconferenza e la collaborazione sui documenti. L'oggetto che transita nella UC è la comunicazione. Gli Utenti vengono identificati con il proprio User Principal Name (UPN), che in ERAP Marche usualmente coincide con l'indirizzo di posta elettronica. L'Utente che invita ospiti esterni a partecipare alla comunicazione (chat o videoconferenza) oppure condivide con tali ospiti l'indirizzo e-mail o il numero telefonico aziendale, si assume la responsabilità di tale invito o condivisione ed è tenuto a comunicare, in anticipo, agli altri partecipanti la presenza di questi ultimi.

Durante l'utilizzo di tali strumenti è opportuno adottare i seguenti comportamenti consoni:

- Adoperare la messaggistica per comunicazioni brevi;
- Controllare frequentemente il proprio stato di presenza e adeguarlo alla propria corrente attività;
- Controllare lo stato di presenza degli utenti con cui si vuole comunicare ed evitare, quando non necessario, di attivare una comunicazione sincrona se l'utente è già impegnato;
- Silenziare il microfono durante gli interventi altrui;
- Utilizzare lo strumento alzata di mano - ove presente – per chiedere la parola, in particolare nelle comunicazioni affollate, onde evitare sovrapposizioni;
- Adoperare gli strumenti adatti per selezionare uno o più utenti a cui rispondere privatamente, qualora non fosse necessario coinvolgere altri all'interno di una discussione di gruppo;
- Specialmente qualora si effettui una videochiamata in luoghi in cui sono presenti persone estranee alla conversazione, evitare inquadrature e registrazioni video o audio che ledano la privacy altrui.

Per la creazione di stanze virtuali di chat o audio/videoconferenza, siti, gruppi e relativi canali di condivisione, è necessario chiedere la preventiva autorizzazione al Settore Informatica e Digitalizzazione.

Il sistema di UC prevede la possibilità di inviare messaggi, effettuare videoconferenze, telefonare e, previo consenso di tutti i partecipanti, registrare ognuna delle suddette comunicazioni. I partecipanti alla comunicazione hanno la responsabilità del proprio comportamento e del rispetto della netiquette, anche qualora supportati tecnicamente dal Settore Informatica e Digitalizzazione tramite Helpdesk; i partecipanti, inoltre, sono responsabili della manutenzione dei documenti e della cancellazione dei dati non più necessari.

La chat è persistente, pertanto ne rimane traccia come da termini di utilizzo. Nel rispetto della normativa in materia di tutela della libertà e dignità dei lavoratori e della normativa unionale e nazionale in materia di protezione dei dati personali, sono attivi sistemi di monitoraggio delle

comunicazioni che consentono di verificare mittente, destinatario, durata/data e stato (ad esempio, per le telefonate, numero chiamato e chiamante con mascheramento delle ultime cifre del numero, durata, chiamata non risposta o rifiutata). Detti sistemi sono destinati esclusivamente all'analisi del tipo di traffico ai fini di reportistica e manutenzione e le relative informazioni (dati aggregati) sono accessibili ai soli amministratori dei sistemi di UC.

2.9 Servizi Cloud e Spazi di condivisione di rete aziendale

Ad integrazione di quanto già disciplinato nell'art. 22 Del Reg. Privacy, qui richiamato integralmente, si dispone quanto segue.

Gli **spazi di condivisione** file server (on premise) o cloud, devono essere utilizzati per la memorizzazione di file ad uso strettamente lavorativo. I file e i documenti di lavoro devono essere obbligatoriamente memorizzati nello spazio di condivisione apposito al fine di impedire la perdita di dati aziendali, a seguito di guasti alle PdL.

In caso di comprovato pericolo per la sicurezza dei sistemi, ERAP Marche potrà procedere anche senza preavviso alla rimozione di file e/o applicazioni presenti negli spazi di condivisione dei Collaboratori, dandone successiva e tempestiva comunicazione agli interessati.

2.9.1 Servizi cloud forniti da aziende terze

L'ERAP Marche fornisce a tutti i Collaboratori il servizio di cloud storage "Microsoft One Drive", accessibile tramite browser, applicazione desktop e mobile sia dalla rete aziendale che dalla rete internet. L'accesso è effettuato mediante le credenziali di dominio e l'utilizzo del servizio è consentito esclusivamente per la memorizzazione di file attinenti all'attività lavorativa. L'installazione e l'utilizzo di altri sistemi di cloud storage concorrenti (ad es. Dropbox, Google Drive, etc.) devono essere preventivamente richiesti con opportuna motivazione e autorizzati dal Settore Informatica e Digitalizzazione.

2.10 Dispositivi di memorizzazione rimovibili (Hard disk, Pen drive USB, etc.)

L'utilizzo di supporti di memorizzazione rimovibili deve essere effettuato con molta cautela ed esclusivamente per le attività lavorative. Al momento della connessione di un dispositivo esterno viene avviata la scansione automatica antivirus, per permettere al sistema di completare la verifica di sicurezza che non può essere interrotta dall'Utente. È inoltre fondamentale che il dispositivo non venga disconnesso durante la scansione, per non danneggiare e rendere illeggibili i dati.

L'utilizzo di dispositivi rimovibili, utile per esempio per effettuare copie di sicurezza o per trasportare file di grandi dimensioni, rimane in ogni caso sotto la responsabilità dell'utilizzatore, che è tenuto a rivolgersi al Settore Informatica e Digitalizzazione per le opportune configurazioni di sicurezza e/o crittografia del dispositivo.

È vietato consegnare a terzi supporti già utilizzati per la memorizzazione di informazioni o di dati personali, anche se cancellati, in quanto è tecnicamente possibile il loro recupero anche dopo l'intervenuta cancellazione.

L'Utente è tenuto a informare immediatamente i dirigenti responsabili della struttura organizzativa di appartenenza, il Settore Informatica e Digitalizzazione e il Responsabile della Protezione dei Dati, anche ai sensi della procedura di gestione delle violazioni di dati personali, di qualsiasi danno, furto o perdita di apparati, software e/o dati in proprio possesso, fatti salvi gli obblighi di denuncia alle autorità competenti.

Alcune raccomandazioni di buon senso:

- I supporti rimovibili (CD, DVD, pen drive, schede di memoria, hard disk rimovibili, etc.) devono essere custoditi con la massima diligenza e riservatezza e non devono essere lasciati incustoditi o facilmente accessibili.
- Nel momento in cui l'Utente non ha più bisogno del supporto, sia esso riscrivibile o non riscrivibile (ad esempio: CD-R, DVD-R, DVD+R, CD-RW, DVD-RW, DVD+RW, pen drive, schede di memoria, hard disk rimovibili, etc.), è tenuto a restituirlo al Settore Informatica e Digitalizzazione.

2.10.1 Copia delle informazioni e gestione supporti strumenti portatili

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

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

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

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

regole di condotta:

- è vietato di copiare, trasferire, o muovere file dai server o NAS (Network Access Storage) interne su PC portatili o supporti removibili, tranne che per esigenze eccezionali e solo se espressamente autorizzato da figure dotate degli opportuni poteri amministrativi (in tal caso, l'autorizzazione deve essere accompagnata da indicazioni utili per la sicurezza delle informazioni);
- non appena cessate tali esigenze, i file devono essere ritrasferiti sui server dell'ERAP Marche, eliminandoli dal dispositivo portatile;
- la memorizzazione dei dati sulle Pen Drive deve essere esclusivamente a carattere temporaneo (possibilmente nell'ordine di poche ore) e le stesse debbono essere oggetto di formattazione immediata dopo l'utilizzo temporaneo del file memorizzato. Le Pen Drive devono essere tassativamente rilasciate senza alcun file al loro interno;
- è fatto comunque divieto di utilizzare supporti rimovibili personali;
- non lasciare mai incustodito un dispositivo portatile, in particolare non lasciare mai sulla scrivania, rendendoli facilmente accessibili, pen drive o HD esterni. Gli stessi debbono essere custoditi in cassetti o armadi chiusi a chiave e comunque gestiti con la stessa accortezza e diligenza delle altre risorse in dotazione;
- deve essere sempre applicata la policy del "bring the device always with you", ovvero non lasciare incustodito un dispositivo, nell'automobile, presso soggetti esterni in area non controllata, in sale riunioni non chiuse a chiave, ecc.;
- non trascrivere informazioni sensibili (login, password, ecc.), né in forma cartacea né in forma elettronica, all'interno di un dispositivo, a meno che questo non avvenga mediante opportuna procedura di crittazione dei dati precedentemente autorizzata e concordata con la dirigenza e/o il Settore Informatica e Digializzazione;
- per i medesimi motivi, lo scambio di informazioni e/o di dati anche all'interno dell'organizzazione dovrebbe avvenire mediante condivisione della risorsa all'interno dei server e/o delle NAS interne, piuttosto che per posta elettronica e/o mediante l'uso di dispositivi removibili;
- non usare dispositivi come Pen Drive per il salvataggio primario di file ovvero per l'editing online invece di usare i supporti interni al PC.

2.11 Strumenti di firma digitale

L'uso del kit di firma digitale, anche remota, è strettamente personale e non cedibile a terzi. Qualora un Collaboratore consegni il kit di firma digitale ad un altro Collaboratore e lo autorizzi a firmare al suo posto, resta totalmente e pienamente responsabile di quanto è stato firmato in quanto il documento risulta a tutti gli effetti firmato dal titolare della firma.

2.12 Comportamento in caso di assenza programmata

In caso di assenza programmata, al fine di garantire la continuità del servizio, il Collaboratore si impegnerà a:

1) rendere disponibile, ove necessario, la relativa documentazione su una share condivisa dell'ufficio;
2) attivare eventualmente la funzione di risposta automatica, utilizzando un messaggio contenente il periodo di assenza e l'eventuale contatto alternativo.

2.13 Comportamenti non consentiti

Sono vietati a tutti i Collaboratori i seguenti comportamenti:

a) l'utilizzo abusivo di credenziali altrui, la cessione a terzi delle credenziali di utilizzo della smart card di firma digitale (o strumento equivalente), l'accesso non autorizzato a risorse informatiche di ERAP Marche e/o lo scambio di comunicazioni mediante falsa identità;
b) l'installazione, sulla PdL in dotazione, di software non coperto da licenza o, comunque, non preventivamente autorizzato dal Settore Informatica e Digitalizzazione;
c) l'utilizzo, per comunicazioni personali, di chat, social network o altri strumenti di comunicazione aziendale messi a disposizione da ERAP Marche;
d) l'utilizzo, la distruzione, l'alterazione o la disabilitazione non autorizzata di file e di ogni altra risorsa informatica;
e) l'allontanamento dalle PdL senza la preventiva adozione di opportune precauzioni di sicurezza (ad es. il blocco della PdL);
f) il mantenimento delle PdL accese al termine della giornata lavorativa, salvo il caso in cui si preveda di dover lavorare da remoto;
g) la modifica delle configurazioni di base dei dispositivi assegnati dall'ERAP Marche senza l'autorizzazione preventiva del Settore Informatica e Digitalizzazione (non è possibile, ad esempio, configurare account privati nel client di posta);
h) l'utilizzo di strumenti volti a eludere i sistemi di protezione.

2.14 Protezione contro furti e danneggiamenti

Tutte le PdL portatili e i dispositivi mobili devono essere custoditi in luogo sicuro, adottando le opportune precauzioni contro il furto delle strumentazioni informatiche e/o dei dati in esse contenuti.

Il Collaboratore è tenuto a informare immediatamente il dirigente responsabile, il Settore Informatica

e Digitalizzazione e, qualora vi sia la possibilità di una violazione di dati personali, altresì il RPD di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso, fermi restando gli obblighi di denuncia alle autorità competenti.

2.15 Abuso e alterazione delle risorse ICT

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

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

2.16 Custodia delle risorse

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

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

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

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

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

2.17 Politica del "Clean Desk" e "Clean Desktop"

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

2.17.1 Regole di condotta per l'applicazione della politica di "Clean Desk" e "Clean Desktop"

È vietato:

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

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

2.17.2 Obblighi specifici per l'applicazione della politica di "Clean Desk" e "Clean Desktop"

- I computer e terminali non debbono essere lasciati collegati o questi devono essere protetti, quando incustoditi, con un salva-schermo e meccanismi di blocco della tastiera controllati con una password o token o con altri meccanismi similari di autenticazione dell'utente.
- Le stampe contenenti informazioni riservate o classificate devono essere rimosse immediatamente dalle stampanti.

- Tutti i computer workstation devono essere bloccati quando l'area di lavoro non è occupata.
- Salvo i casi già citati in cui è previsto di dover lavorare da remoto, tutti i computer workstation devono essere spenti al termine della giornata lavorativa. Nel caso in cui dati ed alle informazioni trattati nella sessione di lavoro abbaino particolare impatto sulla sicurezza e la riservatezza, il computer dovrà essere spento anche durante la giornata se la postazione di lavoro non viene usata per due ore o più.
- Quando la scrivania non è presidiata ed alla fine della giornata di lavoro i documenti devono essere rimossi dalla scrivania e riposti in un cassetto o altro luogo chiuso a chiave.
- Gli armadi contenenti dati personali ed informazioni riservate devono essere mantenuti chiusi e bloccati quando non sono in uso e non sono presidiati a vista.
- Strumenti di accesso quali chiavi digitali, token, smart card, ecc. ecc. (utilizzati per accedere a informazioni riservate o ristrette) non devono essere mai lasciati incustoditi.
- Computer portatili devono essere bloccati con un cavo antieffrazione o chiusi a chiave in cassetti o armadi.
- Il login e la password sono informazioni strettamente riservate che dovranno essere memorizzate, senza trascriverli e mantenerli visibili tramite post-it o altre modalità nella postazione di lavoro e/o in una posizione comunque facilmente accessibile.
- Nel caso di stampa di documenti contenenti dati personali e informazioni riservate gli stessi devono essere immediatamente rimossi dalla stampante.
- I documenti riservati e/o ad accesso limitato, non più necessari, devono essere distrutti nel distruggi documenti e non lasciati senza protezione
- Lavagne contenenti informazioni devono essere cancellate ed i fogli distrutti.
- Bloccare immediatamente i dispositivi informatici portatili come i laptop e tablet subito dopo il loro uso, anche per assenze temporanee molto brevi.
- Trattare i dispositivi di archiviazione di massa come CD-ROM, DVD, o unità USB / Pen Drive come critici e chiuderli sempre in un cassetto o armadio.
- Identificare sempre le Pen Drive utilizzate, in modo che un loro furto possa essere sempre identificato.

2.18 Obbligo alla riservatezza e al segreto professionale

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

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

Nel caso in cui, per disposizioni di legge o di regolamento o per ordine di Autorità competenti, sia necessario inviare delle informazioni a soggetti terzi, dovrà essere preventivamente informata l'ERAP Marche ed anticipatamente concordati tempi e modalità di comunicazione.
La stampa dei messaggi o informazioni deve essere contenuta a quanto strettamente necessario per una corretta consultazione. Di norma, il documento cartaceo deve essere distrutto dopo la consultazione, salvo che esso sia utile per usi tecnici o di documentazione all'interno di specifici dossier.

2.19 Informazioni Riservate e Accordi di Riservatezza

Per informazioni riservate si intendono tutte le informazioni riferite all'ERAP Marche, ai soggetti esterni e a qualsiasi collaboratore coinvolto anche indirettamente, identificate come tali dall'ERAP Marche stessa. A titolo esemplificativo e non esaustivo, esse sono: le informazioni scientifiche e/o tecniche riguardanti procedure, processi e know-how, prototipi realizzati, specifiche e dati, domande di brevetto depositate e ancora segrete, disegni, design e formule, informazioni, notizie, valutazioni, proposte, offerte, progetti, software e sistemi informatici, istanze, domande, osservazioni e quant'altro.
L'informazione può essere di qualsiasi forma, ossia verbale, scritta, informatica, digitale, immagini, suoni, ecc.
L'informazione è sempre classificata come "USO INTERNO" salvo diversa espressa indicazione.
La riservatezza si estende anche a informazioni riguardanti personale, collaboratori, clienti/utenti e fornitori dell'ERAP Marche
Ogni dipendente, collaboratore, fornitore esterno si impegna irrevocabilmente a non divulgare le informazioni riservate riferite all' ERAP Marche. Il soggetto esterno si impegna inoltre affinché anche i suoi dipendenti e consulenti esterni garantiscano la già menzionata riservatezza delle informazioni.
Gli obblighi di non divulgazione e diffusione delle informazioni riservate sono previsti nel contratto individuale di lavoro per il personale interno e in apposite *Non Disclosure Agreement* (NDA) per i collaboratori e i fornitori esterni. Tali accordi vengono documentati e riesaminati periodicamente.
Tutti gli obblighi al segreto e alla riservatezza a cui sono tenuti i dipendenti e i collaboratori dell'ERAP Marche rimangono in essere e validi anche dopo la cessazione del rapporto di lavoro o del rapporto di collaborazione.

2.20 Utilizzo condiviso delle risorse ICT

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

2.21 Obbligo di condivisione ed informazione

Tutto il personale, a qualsiasi livello, e tutti i collaboratori hanno l'obbligo di comunicare al proprio responsabile e/o alSettore Informatica e Digitalizzazione, azioni, situazioni, rischi, procedure (interne e/o esterne), stati di fatto, interazioni, attività o altro che possano comportare un rischio per la sicurezza e la riservatezza dei dati e delle informazioni.

3 Controlli e monitoraggi

ERAP Marche imposta la propria azione di monitoraggio e controllo sui sistemi informatici messi a disposizione per lo svolgimento dell'attività lavorativa nel rispetto della normativa vigente e sul presupposto di un utilizzo responsabile degli stessi da parte dei Collaboratori, adottando in ogni caso le soluzioni tecnologiche idonee a garantire i profili di sicurezza dei sistemi informativi e dei dati gestiti.

A tal fine, ERAP Marche utilizza sistemi automatizzati per la gestione centralizzata dei cosiddetti "file di log", che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la funzionalità e la sicurezza degli apparati informatici di ERAP Marche e delle informazioni ivi contenute.

I file di log relativi alla navigazione in internet sono registrati e conservati per le suddette finalità di funzionalità e sicurezza, in conformità alla normativa vigente e alle disposizioni adottate al riguardo da ERAP Marche (vedi Appendice B al Reg. Privacy).

Nel caso di eventi anomali e/o pregiudizievoli per la sicurezza informatica, i file di log relativi alla navigazione possono essere esaminati dagli amministratori di sistema per l'individuazione del problema tecnico e l'adozione delle necessarie misure conseguenziali. In ogni caso, tutti i controlli di funzionalità e monitoraggio avvengono nel rispetto di quanto previsto dal CAD, dalle norme in materia di tutela della libertà e dignità dei lavoratori, della normativa unionale e nazionale in materia di protezione dei dati personali.

L'amministratore di sistema, nel caso in cui rilevi anomalie o configurazioni non corrette delle PdL, può provvedere a isolare immediatamente l'origine dell'anomalia o del malfunzionamento anche senza preavvisare il Collaboratore, per salvaguardare la sicurezza e l'integrità dei sistemi informativi di ERAP Marche. In tal caso, verrà data successiva informativa al Collaboratore sui motivi dell'avvenuto intervento sulla PdL da parte dell'amministratore di sistema.

Le predette attività sono svolte nel rispetto dei principi di gradualità, pertinenza e non eccedenza stabiliti dal Garante per la protezione dei dati personali nonché dei diritti e delle libertà fondamentali dei lavoratori, sempre mediante funzionalità consentite dalla normativa vigente.

3.1 Ruolo degli amministratori delle risorse tecnologiche condivise e delle applicazioni

Gli Amministratori delle risorse tecnologiche condivise e delle applicazioni svolgono le attività necessarie per garantire la salvaguardia del sistema informativo e delle applicazioni conformemente alle politiche e alle istruzioni impartite dall'ERAP Marche e nel rispetto della normativa vigente con particolare riferimento alla protezione dei dati personali.
Qualora si renda necessario procedere a operazioni finalizzate al ripristino della funzionalità del Sistema informativo comportanti l'accesso a cartelle, file o archivi di altri Collaboratori, gli Amministratori sono tenuti a preavvisare gli interessati, limitando il proprio intervento a quanto strettamente necessario.

3.2 Tutela riservatezza, integrità, disponibilità e resilienza della rete telematica – Backup

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

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

I pc collegati alla rete di ERAP Marche sono adeguati automaticamente agli ultimi aggiornamenti critici e di sicurezza, sia per il sistema operativo che per il software in dotazione.
L'utente che si collega alla sua postazione di lavoro non può avere i diritti di amministratore locale. Attraverso l'utilizzazione di appositi software centralizzati, sono individuate, da remoto, eventuali anomalie ed irregolarità, autorizzando i soggetti competenti (amministratori di sistema, tecnici autorizzati e referenti informatici) a:

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

3.3 Separazione dati anagrafici e particolari -

pseudonimizzazione, cifratura, minimizzazione

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

Il Settore Informatica e Digitalizzazione supporta ciascun dirigente nell'adozione, se necessario, di misure di pseudonimizzazione, cifratura, minimizzazione ed in ogni altra tecnica di anonimizzazione dei dati trattati, con riferimento anche al parere 10/04/2014 del gruppo ex art.29 della direttiva 95/46.

3.4 Verifica adeguatezza al principio della "Privacy by design"

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

3.5 Cessazione dei servizi

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

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

f) in ogni altro caso in cui sussistono ragionevoli evidenze di una grave violazione dei propri obblighi da parte del Collaboratore.

3.6 Sistema dei controlli

3.6.1 Gradualità

Ad integrazione di quanto già disciplinato nell'art. 28 Del Reg. Privacy, qui richiamato integralmente, si dispone quanto segue.

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

1) analisi aggregata del traffico di rete riferito all'intera Rete Informatica o a sue aree (reparto, servizio, ecc.), rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni) dei dati memorizzati sui server a livello di intera struttura lavorativa (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) dei dati memorizzati su client e relativa pertinenza con l'attività lavorativa;
2) emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti interni, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
3) in caso di successivo permanere di una situazione non conforme e in caso di abusi singoli e reiterati, si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro. Sarà possibile procedere con un'analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro e sugli strumenti informatici in dotazione al singolo lavoratore o collaboratore, alle condizioni sottoindicate. In caso di accertati abusi si procederà anche alla segnalazione all'Ufficio Provvedimenti Disciplinari.

3.6.2 Controlli sui dispositivi in dotazione ai Collaboratori

L'ERAP Marche può procedere a controlli sull'attività dei Collaboratori, nei limiti consentiti dalle norme di legge e contrattuali e nel rispetto dei diritti dei lavoratori, per le seguenti finalità:

- verifica dell'integrità della propria infrasruttura Informatica;
- verifica dell'ottemperanza di disposizioni di legge e contrattuali;
- verifica del rispetto delle disposizioni relative alla sicurezza informatica ed alla protezione dei

dati personali e di quanto previsto dal presente documento;

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

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

3.6.3 Controlli per finalità tecniche e/o amministrative

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

- motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.);
- controllo o programmazione dei costi;
- comprovate esigenze manageriali o lavorative (ad es. accesso al computer del Collaboratore per reperire file necessari all'attività lavorativa che siano conservati esclusivamente "in locale" su detto dispositivo, nel caso di assenza non programmata del Collaboratore);
- permettere il libero accesso alle informazioni tanto della rete internet che della posta elettronica anche all'Autorità Giudiziaria richiedente.

3.6.4 Accesso da remoto alla PdL da parte del Settore Informatica e Digitalizzazione

Per motivi di assistenza, manutenzione, ricerca virus, attività di indagine sui malfunzionamenti, ricerca di anomalie o altre esigenze dell'organizzazione, il Settore Informatica e Digitalizzazione può accedere da remoto sui dispositivi collegati alla rete interna o dall'esterno mediante connessione VPN.

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

4 Responsabilità e sanzioni

La violazione del presente disciplinare e dei Codici di comportamento del personale può comportare l'applicazione delle sanzioni disciplinari previste dal decreto legislativo 30 marzo 2001, n. 165 e s.m.i., dai contratti collettivi applicabili al personale in servizio e dal singolo contratto di lavoro.

Resta ferma la responsabilità civile, penale e contabile di ogni Collaboratore per fatti illeciti e/o danni derivanti da usi non consentiti della Rete o degli strumenti informatici messi a disposizione da ERAPMarche, anche alla luce delle prescrizioni contenute nel presente disciplinare.

5 Disposizioni finali

La presente policy è vincolante per tutti i Collaboratori dell'ERAP Marche.

È applicabile anche agli organi di indirizzo politico che utilizzano strumenti informatici dell'ERAP Marche, fatta eccezione per le disposizioni sanzionatorie e disciplinari.

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

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

Ai fini della sua piena conoscibilità da parte di tutti gli interessati, la presente policy viene anche pubblicata nel canale Privacy del gruppo ERAP Marche sulla piattaforma Microsoft Teams.