ALLEGATO A

AL DECRETO DEL PRESIDENTE DELLA PROVINCIA N. 146 DEL 3/10/2019

REGOLAMENTO SULL'UTILIZZO DELLA POSTAZIONE DI LAVORO E DEGLI STRUMENTI INFORMATICI CON RIGUARDO ALLA PROTEZIONE E LIBERA CIRCOLAZIONE DEI DATI PERSONALI AI SENSI DEL GDPR REGOLAMENTO EUROPEO 679/2016

SOMMARIO

Capo I - Introduzione

Articolo 1 - Premessa

Obiettivo del presente Regolamento, è di preservare la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni a tutela della dignità delle persone fisiche e delle libertà fondamentali. Tale obiettivo si inserisce nel contesto della generale disciplina in materia di Privacy e nel sistema normativo che regola l'organizzazione, i processi e le funzioni dell'Ente Provincia.

Le risorse informatiche e telematiche messe a disposizione della Provincia di Ancona costituiscono uno dei suoi punti di forza, ma nello stesso tempo, possono essere fonte di rischio per la sicurezza delle informazioni trattate e per l'immagine della Provincia di Ancona stessa. Per questo motivo il loro utilizzo deve sempre ispirarsi a criteri di liceità, correttezza e trasparenza.

L'individuazione di regole precise e chiare per l'utilizzo degli strumenti informatici e il trattamento dei dati personali e istituzionali della Provincia di Ancona rappresenta un passaggio obbligato per assicurare una ottimale gestione delle funzioni dell'Ente.

Sono questi gli elementi che, nel contesto della disciplina in materia di privacy, hanno indotto la Provincia di Ancona ad elaborare ed adottare il presente Regolamento, che sostituisce il precedente Regolamento "sull'ordinamento generale degli uffici e dei servizi e della struttura organizzativa dell'ente – disciplinare sull'utilizzo degli strumenti informatici con riguardo alla disciplina della tutela dei dati personali" approvato con deliberazione di Giunta Provinciale n. 565 del 07/12/2007.

Articolo 2 - Tutela del lavoratore

Il luogo di lavoro è una formazione sociale rispetto alla quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità di ciascuno in modo da garantire, in una cornice di reciproci diritti e doveri, l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali.

Articolo 3 - Scopo, campo di applicazione e destinatari

Lo scopo del presente Regolamento è quello di definire un insieme di norme comportamentali a cui tutti gli utenti interni ed esterni che operano per la Provincia di Ancona devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni.

Il presente Regolamento è realizzato in conformità a quanto previsto dal Decreto Legislativo n. 196/2003 così come modificato ed integrato dal D. Lgs. 101/2018- Codice in materia di protezione dei dati personali, dal Regolamento Europeo n. 2016/679 – Regolamento Generale sulla Protezione dei Dati (da ora "RGPD") e dai Provvedimenti del Garante.

Il presente Regolamento è destinato ai seguenti utenti (da ora "Utenti"):

a) Utenti interni:

    1) Segretario e Dirigenti

2) Dipendenti a tempo determinato e indeterminato

3) collaboratori coordinati e continuativi

4) personale in distacco o [o in comando] da altri enti

5) consulenti, tirocinanti e collaboratori occasionali

b) Utenti esterni:

1) collaboratori a qualsiasi titolo di imprese fornitrici di beni, servizi o lavori che realizzano opere in favore della Provincia di Ancona

2) personale che opera presso la Provincia di Ancona in forza di convenzioni o accordi inter-istituzionali

3) visitatori e ospiti di vario genere

Capo II - Definizioni

Articolo 4 - Definizioni tratte dal RGPD

Il presente regolamento recepisce le definizioni riportate nell'art. 4 del RGPD e ne riporta di seguito il contenuto.

a) Riguardo all'oggetto della normativa e del presente regolamento:

1) **Trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

2) **Dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

3) **Dati genetici:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

4) **Dati biometrici**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

5) **Dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

6) **Dati Particolari** (o categorie particolari di dati): dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

7) **Archivio**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

b) Riguardo ai soggetti della normativa e del presente regolamento:

1) **Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

2) **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

3) **Destinatario:** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

4) **Terzo**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

5) **Utenti o incaricati o addetti**: il RGPD non definisce in maniera diretta questa categoria ma, dalla definizione di Terzo si evince che esse siano le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile; di seguito vengono definiti “Utenti”;

c) Riguardo ad altri elementi fondamentali previsti dalla normativa e ripresi dal presente regolamento:

1) **Profilazione:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

2) **Pseudonimizzazione**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e

organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

3) Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

4) Data breach: qualsiasi violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Articolo 5 - Altre definizioni

Sono di seguito riportate alcune altre definizioni utili alla corretta gestione dei processi di trattamento dei dati personali.

a) Badge: tesserino con chip elettronico o con banda magnetica utilizzato per il riconoscimento e la marcatura temporale.

b) Strumenti informatici: stampanti, laptop, computer da tavolo, telefoni fissi, smartphone, tablet, e-book reader, telecamere IP, e, in generale, qualsiasi dispositivo in grado di connettersi a una rete IP.

c) Data Center: locale ad accesso limitato che ospita i server, i sistemi di calcolo e i dispositivi di networking, oltre che i sistemi di storage su cui sono residenti i dati.

d) Dominio: sistema centralizzato di autenticazione e di autorizzazione all'accesso alle risorse telematiche dell'Ente che permette una gestione centralizzata degli utenti e delle risorse informatiche aumentando la sicurezza e l'affidabilità del sistema IT.

e) Cloud pubblico: servizi di elaborazione e di conservazione dati offerti da provider di terze parti tramite la rete Internet pubblica e disponibili per chiunque voglia usarli o acquistarli.

f) Cloud privato: servizi di elaborazione e conservazione dati interno all'azienda. In questo modello le aziende realizzano un ambiente di cloud computing che rimane completamente all'interno del data center, e che consente di mantenere i dati dentro la propria struttura operativa, risolvendo la questione riguardante il problema della privacy e della sicurezza che costituiscono punti critici dei cloud pubblico.

Capo III - Modello organizzativo

Articolo 6 - Classificazione delle informazioni nella Provincia di Ancona

La Provincia di Ancona classifica il proprio patrimonio informativo (costituito da tutti i dati e le informazioni trattati nei diversi processi, tra i quali anche i dati personali) secondo i seguenti criteri:

a) **Dati e informazioni pubbliche (DP)**: sono le informazioni liberamente trattabili da Utenti attraverso i mezzi di comunicazione messi a disposizione della Provincia di Ancona (sito internet, pubblicazioni, comunicati, ecc.). Queste informazioni non richiedono da parte dell'Utente particolari attenzioni di riservatezza. La divulgazione di tali informazioni non presenta implicazioni per la Provincia di Ancona in quanto si tratta di informazioni pubbliche che possono essere diffuse.

b) **Dati e informazioni interne (DI)**: sono le informazioni che possono essere trattate dagli Utenti esclusivamente all'interno dei processi e del contesto organizzativo della Provincia di Ancona attraverso i canali istituzionali messi a disposizione della Provincia di Ancona (e-mail, intranet), aree di scambio su server e computer, ecc.). Queste informazioni richiedono da parte dell'Utente una particolare attenzione nel trattamento, in quanto la loro divulgazione rappresenta una violazione dei vincoli di riservatezza ai quali è legato ogni Utente con un possibile impatto legale (per esempio, violazione della privacy), a meno di essere rielaborate in modo da essere declassate a livello pubblico.

c) **Dati e informazioni riservate(DR)**: sono le informazioni che possono essere trattate da gruppi di Utenti autorizzati in virtù del ruolo e di una precisa finalità di trattamento individuata dal Titolare o dal Responsabile del trattamento. Tali informazioni devono essere comunicate solo ad Utenti legittimati, valutando lo strumento di comunicazione più appropriato messo a disposizione dalla Provincia di Ancona in quanto la loro diffusione può avere un rilevante impatto legale (per esempio, violazione della privacy), d'immagine e di operatività per la Provincia di Ancona.

d) **Dati e informazioni strettamente riservate(DS)**: sono le informazioni che possono essere trattate esclusivamente da determinati Utenti in base al ruolo ed alle responsabilità ricoperte nella Provincia di Ancona. La divulgazione di tali informazioni può produrre gravi danni legali (per esempio, violazione della privacy), di immagine e di operatività per la Provincia di Ancona.

Articolo 7 - Informazioni relative ai trattamenti di propria competenza

La Provincia di Ancona, in ossequio a quanto previsto dall'art. 30 del RGPD, ha elaborato ed approvato (giusto decreto del Presidente n. 30 del 21/02/2019) il registro delle attività di trattamento dei dati personali, un documento informatico nel quale sono descritte le attività di ogni singolo trattamento, i tipi di dati trattati, i tipi di interessati, i destinatari, le misure di sicurezza a cui il trattamento è sottoposto.

Il documento è presente sulla intranet dell'Ente (http://stamira/Documentazione/privacy/home.htm) e deve essere costantemente consultato da ciascun Utente per essere aggiornato circa le caratteristiche dei trattamenti affidati Può essere divulgato all'esterno della Provincia purché vengano omesse le misure di sicurezza ad esso relative in quanto le informazioni ivi contenute, possono, in mani sbagliate, costituire un elemento di rischio alla sicurezza dei dati.

Articolo 8 - Modello organizzativo di responsabilità privacy

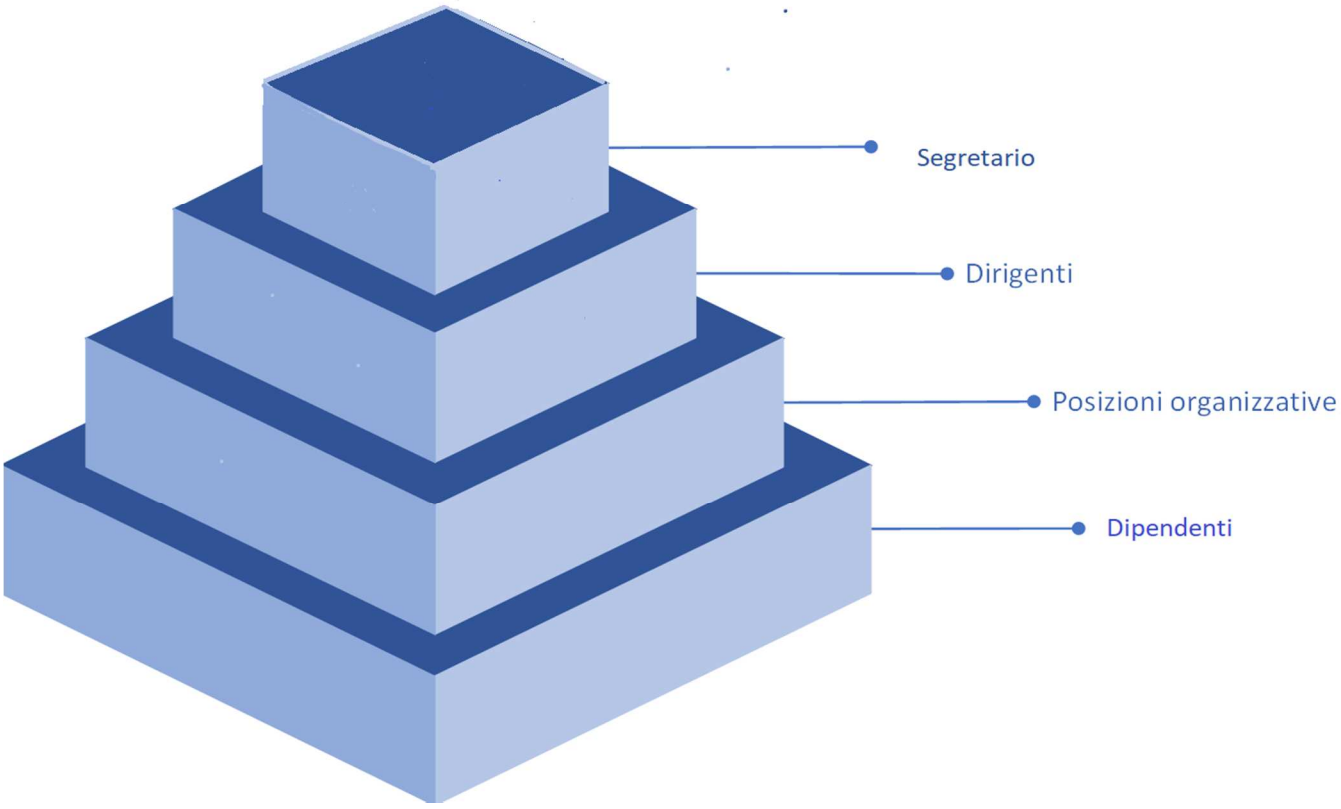
Nell'ambito della conformità al RGPD e sulla base del proprio organigramma, la Provincia di Ancona ha definito e formalizzato un Modello Organizzativo di responsabilità privacy finalizzato al corretto trattamento dei dati personali.

Tale Modello Organizzativo prevede che ci sia una equivalenza tra le responsabilità operative attribuite a ciascun titolare di incarico dirigenziale e di posizione organizzativa e le conseguenti responsabilità sui trattamenti effettuati in termini di rispetto della normativa in materia di privacy.

Pertanto ogni superiore deve mettere in atto misure tecniche e organizzative adeguate a garantire ed essere in grado di dimostrare che le attività di trattamento proprie e dei propri sottoposti sono effettuate nel rispetto di quanto disposto dalla normativa sulla privacy e da questo regolamento e sarà pertanto ritenuto responsabile di ogni violazione.

Al di là del Modello Organizzativo relativo alle responsabilità privacy di cui sopra, tutti coloro che siano a capo di un progetto che contempla il trattamento di dati personali - d'intesa con il Titolare e per il tramite del Responsabile della Prevenzione, della Corruzione e della Trasparenza (RPCT) e con il Responsabile della Protezione dei Dati (RPD o DPO) – sono tenuti ad adottare una policy *ad hoc* configurata sulle specifiche esigenze del caso (c.d. Privacy by Design).

Rappresentazione grafica delle responsabilità in merito alla legalità e alla conformità al GDPR dei trattamenti effettuati



Capo IV - Regole di comportamento

Sezione 1 - Principi generali

Articolo 9 - Principi generali del trattamento

Trattare un dato personale vuol dire compiere qualunque operazione o complesso di operazioni realizzate su un dato personale ed effettuate anche senza l'ausilio di strumenti elettronici. Il trattamento di un dato personale, per essere lecito, corretto e trasparente, deve sempre avvenire secondo alcuni principi generali a tutela della privacy, che possono essere considerati vincoli inscindibili al trattamento dei dati personali. È importante assicurarsi sempre se questi vincoli siano stati rispettati per avere la certezza che la privacy di una persona sia rispettata.

In particolare quando avviene un trattamento di dati personali devono sempre essere rispettati i seguenti principi generali:

a) **dignità dell'interessato**, cioè della persona fisica di cui si stanno trattando i dati personali.

b) **principi di liceità, correttezza e trasparenza:** i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato, in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentali. Quanto alla trasparenza, è fatto obbligo a tutti gli Utenti di fornire agli interessati all'atto della raccolta dei dati (sia essa orale, tramite modulistica, o in qualunque altra forma) le informative a tutela dei dati personali predisposte dall'Ente per ciascun specifico trattamento; tutte le informazioni destinate al pubblico o all'interessato devono essere concise, facilmente accessibili e di facile comprensione; il linguaggio utilizzato deve essere semplice e chiaro.

c) **principio di limitazione della finalità:** gli scopi del trattamento devono essere determinati, espliciti e legittimi, e successivamente trattati in un modo che non sia incompatibile con tali scopi (salvi gli ulteriori trattamenti per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica o storica, o per fini statistici).

d) **principio di minimizzazione dei dati:** i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Nello specifico, i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'uso di dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi o altre opportune modalità che permettano di identificare l'interessato solo in caso di necessità ('principio di necessità').

e) **principio di esattezza**: i dati trattati devono essere esatti e, se necessario, aggiornati, pertanto devono essere adottate tutte le misure ragionevoli per cancellare o rettificare i dati inesatti rispetto alle finalità per le quali sono trattati.

f) **principio di limitazione della conservazione**: i dati trattati devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario al conseguimento degli scopi per cui sono raccolti e trattati (salvo specifici obblighi di legge, trattamenti di archiviazione nel pubblico interesse o per finalità di ricerca scientifica o storica, o per fini statistici).

g) **principio di integrità e riservatezza**: i dati devono essere trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dal rischio di perdita, distruzione e danno accidentale.

h) **principio di protezione per impostazione predefinita (Privacy by Default):** nel caso in cui non siano state fornite istruzioni specifiche o in caso di dubbio su come svolgere le singole attività di trattamento, devono essere trattati solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, non devono essere resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona interessata. Eventuali eccezioni o comportamenti difformi, anche qualora siano valutati necessari ai fini del compimento dell'attività lavorativa, prima di essere posti in essere devono essere concordati con il proprio superiore gerarchico ed il Responsabile per la protezione dei dati personali.

i) **principio di protezione fin dalla progettazione (Privacy by Design):** Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del RGPD e del presente regolamento e tutelare i diritti degli interessati.

Sezione 2 - Regole relative ai locali

Articolo 10- Gestione dei locali e delle risorse fisiche

Tutti i locali e tutte le risorse fisiche della Provincia di Ancona devono essere utilizzati e custoditi con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa ed un adeguato livello di sicurezza delle informazioni, attenendosi al presente Regolamento per garantire la sicurezza fisica di aree ed *asset* della Provincia di Ancona.

Articolo 11 - Accesso agli uffici ed aree protette

L'accesso agli uffici, alle aree protette, alle aree riservate ed agli archivi cartacei, è permesso agli Utenti autorizzati muniti di badge personale, in base a precise e motivate esigenze lavorative.

I visitatori e gli ospiti di vario genere potranno avere accesso agli uffici della Provincia di Ancona esclusivamente se accompagnati dall'addetto alla portineria.

Articolo 12 - Accesso ai locali del Data Center

L'accesso ai locali del Data Center della Provincia di Ancona è permesso esclusivamente a personale autorizzato munito della relativa chiave.

In via eccezionale e per breve tempo, nel Data Center è consentito l'accesso anche a visitatori e ospiti di vario genere, purché autorizzati e accompagnati da personale della Provincia di Ancona autorizzato addetto al controllo del Data Center medesimo. I visitatori e gli ospiti di vario genere dovranno essere adeguatamente istruiti da predetto personale autorizzato in merito alle caratteristiche dell'ambiente, ai rischi presenti, alle norme comportamentali previste e alle procedure da attuare per prevenire o gestire situazioni di emergenza e di rischio.

Per motivi di sicurezza e per conservare la temperatura costante di esercizio, tutti i varchi di accesso devono restare aperti solamente per il tempo strettamente necessario al passaggio di persone e materiali.

Articolo 13 - Riprese video-audio-fotografiche all'interno dei locali dell'ente

Qualsiasi ripresa video-audio-fotografica deve essere realizzata rispettando i diritti delle singole persone coinvolte.

Utenti interni: per ragioni connesse alla propria attività lavorativa le riprese video-audio-fotografiche devono essere autorizzate dal proprio superiore gerarchico. Tali riprese possono essere utilizzate esclusivamente per finalità lavorative e non possono essere divulgate al di fuori del contesto istituzionale in cui sono state realizzate.

Al di fuori di questa casistica è vietato effettuare riprese video-audio-fotografiche in qualunque area della Provincia di Ancona, salvo preventiva e formale autorizzazione del proprio superiore gerarchico.

Gli Utenti interni potranno essere fotografati e/o ripresi in occasione di eventi, seminari e momenti di formazione. In questi casi, le immagini e le riprese potranno essere utilizzate per scopi e comunicazioni istituzionali.

Utenti esterni: è vietato effettuare riprese video-audio-fotografiche in qualunque area della Provincia di Ancona. Eventuali eccezioni devono essere autorizzate dal Dirigente o suo delegato. L'Utente interno referente della visita è tenuto a far rispettare queste prescrizioni.

Sezione 3 - Regole relative alla gestione della postazione di lavoro e dei dati in generale

Articolo 14 - Postazioni di lavoro

L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi.

Scrivania pulita. La propria scrivania deve essere mantenuta in ordine, verificando di non lasciare documenti e atti riservati senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

Articolo 15 – Dispositivi elettronici personali

Ai sensi dell'art. 12, comma 3-bis del D.Lgs. 82/2005, la Provincia di Ancona favorisce l'uso da parte degli Utenti interni di dispositivi elettronici singolarmente assegnati o, di dispositivi di proprietà personalizzabili, al fine di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo e nel rispetto del presente regolamento.

Ai sensi dell'art. 8-bis del D.Lgs. 82/2005, la Provincia di Ancona favorisce la disponibilità di connettività alla rete Internet a disposizione degli Utenti esterni nel rispetto degli standard e delle modalità fissate dall'AgID e del presente regolamento.

Articolo 16 - Misure fisiche di custodia di documenti e atti cartacei

I dati cartacei ed i supporti cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi in armadi o cassettiere del contesto organizzativo in cui si opera. Tutti gli archivi sono ad accesso limitato, per cui è possibile accedervi nei limiti della necessità per prelevare e riporre i documenti necessari per lo svolgimento delle mansioni lavorative. I documenti dovranno essere riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa negli appositi archivi.

Gli archivi di documenti e atti contenenti dati particolari dovranno essere custoditi in armadi chiusi a chiave.

L'**eliminazione fisica** di ogni documento cartaceo o supporto informatico contenente dati e informazioni istituzionali e/o personali deve essere effettuata solo utilizzando gli appositi strumenti e nel rispetto di quanto previsto nel Manuale di Gestione documentale dell'Ente.

Si raccomanda di non lasciare documenti incustoditi presso i **dispositivi di stampa**. Non lasciare accedere alle stampe persone non autorizzate; se la stampante non si trova sulla propria scrivania, recarsi quanto prima a ritirare le stampe. Si raccomanda, inoltre, di distruggere personalmente le stampe quando non servono più.

Articolo 17 - Gestione dei dati personali e istituzionali

Ogni Utente è responsabile dei dati e delle informazioni delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità ed il corretto utilizzo.

I dati e le informazioni potranno essere comunicati a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.

È vietata la comunicazione di dati e informazioni verso terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale ed al *know-how* ed alla efficacia ed efficienza dell'attività dell'Ente o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.

È assolutamente vietata la divulgazione a terzi di informazioni riservate, confidenziali o comunque di proprietà del Titolare. In caso di violazione, il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.

Si ricorda, inoltre, che la diffusione illecita di dati e informazioni potrebbe configurare, oltre alla violazione del presente Regolamento, la violazione di norme con conseguenze sia civili che penali a carico del responsabile dell'illecita diffusione, nonché come violazione della normativa che regola il rapporto di lavoro.

In caso di furto o smarrimento di fascicoli o atti contenenti dati personali l'Utente deve informare immediatamente per iscritto il proprio Responsabile di Area ed il Dirigente. Dovrà altresì informare il Responsabile Protezione Dati al seguente indirizzo di posta elettronica privacy@provincia.ancona.it .

Sezione 4 - Regole relative agli strumenti informatici

Articolo 18 - Strumenti informatici

L'utilizzo degli strumenti informatici in dotazione è di carattere professionale. In deroga a tale principio Provincia di Ancona autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale. Lo spazio dello strumento affidato utilizzato a fini "privati" (ad esempio dislocazione di file dati, foto o filmati), dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all'utilizzo professionale.

Tutti gli strumenti dovranno essere bloccati e protetti da password, se lasciati incustoditi.

Gli strumenti dovranno essere automaticamente spenti o messi in modalità a basso consumo se non usati per più di un'ora, a meno di motivate esigenze legate all'attività lavorativa.

Articolo 19 - Custodia degli strumenti informatici

Gli strumenti informatici di proprietà della Provincia di Ancona devono essere custoditi dall'Utente con cura e diligenza prevenendo possibili danneggiamenti che ne compromettano il corretto funzionamento ed evitando di lasciarli incustoditi in ambienti pubblici.

In caso di furto, perdita o danneggiamento di beni contenenti dati personali, l'Utente dovrà informare immediatamente, preferibilmente per iscritto, il Responsabile di Area ed il Dirigente. Dovrà altresì informare il Responsabile Protezione Dati al seguente indirizzo di posta elettronica privacy@provincia.ancona.it. L'utente dovrà altresì raccordarsi con l'area informatica e telematica e con l'area affari generali ai fini dell'attivazione delle conseguenti denunce, degli atti di scarico attrezzature e delle coperture assicurative.

L'accesso agli strumenti informatici di proprietà della Provincia di Ancona è consentito solo ai dipendenti dell'Ente; l'eventuale accesso di terzi è consentito solo se previamente autorizzato.

L'Utente interno di cui all'art.12, comma 3-bis del D.Lgs. 82/2005 che usa un proprio dispositivo elettronico contenente dati personali della Provincia di Ancona, nel caso di furto, perdita o danneggiamento del dispositivo dovrà immediatamente informare per iscritto il Responsabile Protezione Dati al seguente indirizzo di posta elettronica: privacy@provincia.ancona.it.]

Articolo 20 - Gestione delle credenziali di accesso e delle password

Le credenziali di autenticazione per l'accesso al dominio, alla rete, ai pc e per altri servizi vengono assegnate dall'Amministratore di Sistema e consegnate all'Utente; esse consistono in un codice per l'identificazione dell'Utente (username), associato ad una parola chiave (password) riservata che dovrà essere nota solo all'Utente. La responsabilità della custodia della password è affidata all'Utente e questi dovrà modificarla:

a) al primo accesso;

b) alla scadenza, ogni 6mesi;

c) ogni qual volta l'utente sospetti che la parola chiave abbia perso la sua caratteristica di riservatezza (perché ad esempio conosciuta da qualcun'altro o facilmente individuabile).

Ogni Utente è responsabile della sicurezza e di qualunque operazione effettuata utilizzando le proprie credenziali. È proibito accedere alla rete e ai programmi o ai sistemi (pc, server, ecc.) con credenziali diverse da quelle fornite o in maniera anonima. È altresì vietato utilizzare credenziali diverse da quelle di dominio per accedere ai PC (ad esempio, con le credenziali di utenti locali del PC).

In particolare sono **vietati** i seguenti comportamenti:

a) Comunicare ad altri la propria password. Lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare le sue risorse o possa farlo a suo nome.

b) Scrivere la password in posti dove possa essere letta facilmente, soprattutto vicino al computer. Occorre fare attenzione, inoltre, che nessuno veda i caratteri digitati sulla tastiera quando si immette la password.

c) Scegliere password deboli, che si possano trovare in un "dizionario" cioè in una raccolta di password più utilizzate (un esempio di password da non usare mai è presente a questo collegamento:

https://www.smartworld.it/informatica/peggiori-password-piu-usate-2017.html). Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.

d) Usare il proprio nome utente o i nomi di parenti o di animali domestici o altre informazioni personali, specialmente se presenti sui social network.

Le password dovranno essere generate dagli Utenti seguendo i seguenti criteri:

a) non dovranno contenere al loro interno riferimenti personali (nome proprio o di un parente, date di nascita, ecc.);

b) dovranno essere diverse da quelle generate in precedenza;

c) dovranno essere composte da almeno 8 caratteri;

d) dovranno essere composte utilizzando contemporaneamente almeno tre delle quattro tipologie dei seguenti caratteri:

1) almeno una lettera maiuscola

2) almeno una lettera minuscola

3) almeno un numero

4) almeno un carattere non alfanumerico (segni di interpunzione, spazi o altri simboli grafici)

Articolo 21 - Gestione e protezione dei dati digitali

L'accesso ai dati è consentito nei limiti della propria funzione organizzativa e della propria attività lavorativa.

Le cartelle U:\ e V:\(gruppi) sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia inerente all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale incaricato.

Il **cloud privato** http://calipso.provincia.ancona.it/ permette l'accesso universale ai file via Web e consente di condividere file su un server aziendale senza coinvolgere fornitori terzi di servizi per garantire la massima privacy e la massima riservatezza dei dati. Il sistema supporta il lavoro collaborativo di gruppi di lavoro misti composto di utenti interni e di esterni alla Provincia, che possono o meno essere membri del cloud. I files possono essere lavorati in modalità off-line ovvero senza connessione, e la piattaforma si occuperà di sincronizzare tutti i dispositivi che condividono le risorse alla prima connessione ad internet. I Files e le cartelle saranno condivisibili in modo autonomo dall'utente con altri membri del cloud e via email per gli utenti esterni non membri. I dati contenuti in Calipso non sono soggetti a salvataggio da parte del personale incaricato. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.

I dati contenuti sui singoli pc non sono soggetti a salvataggio da parte del personale incaricato. Pertanto la responsabilità del salvataggio di dati ivi contenuti è pertanto a carico del singolo Utente.

Il backup dei principali server di rete viene effettuato dagli Amministratori di Sistema. Gli Utenti che trattengono dati della Provincia di Ancona in aree per cui non è previsto backup sono responsabili del salvataggio degli stessi e di eventuali danni alla Provincia di Ancona o a terzi anche di natura civilistica causati dalla loro perdita o sottrazione.

Proprio per garantire la sicurezza e l'integrità delle informazioni presenti sui sistemi informatici della Provincia di Ancona, non è possibile garantire in maniera assoluta, in caso di controlli, la segretezza delle informazioni personali eventualmente ivi contenute.

La memorizzazione temporanea di dati su strumenti informatici privati è consentita a patto che i suddetti strumenti siano protetti in modo da non consentire l'accesso di estranei non autorizzati.

È vietato il salvataggio di dati e informazioni di carattere istituzionale in sistemi di ***cloud pubblica*** non autorizzati dagli Amministratori di Sistema (Dropbox, iCloud, Onedrive, ecc.).

Ai sensi dell'art. 47, comma 1, del D.Lgs. 82/2005 è ammessa la trasmissione dalla Provincia di Ancona esclusivamente ad altra pubblica amministrazione di documenti resi disponibile sul **cloud privato** http://calipso.provincia.ancona.it/ previa comunicazione delle modalità di accesso telematico agli stessi.

Articolo 22 - Gestione della posta elettronica

L'assegnazione di una casella di posta elettronica della Provincia di Ancona (da ora "e-mail Provincia di Ancona) è di carattere professionale. In deroga a tale principio la Provincia di Ancona autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale. Lo spazio della risorsa affidata utilizzato a fini "privati" dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all'utilizzo professionale.

L'Ente, in conformità alla disciplina in materia di privacy, prevede che ad ogni messaggio in uscita sia automaticamente aggiunto un breve testo di avviso al ricevente della natura potenzialmente riservata del messaggio.

Gli Utenti dell'e-mail Provincia di Ancona sono responsabili dell'utilizzo della stessa e devono mantenere un corretto comportamento nell'utilizzo della posta elettronica. In particolare, gli Utenti devono seguire le seguenti disposizioni:

a) non inviare né conservare messaggi di posta elettronica e/o allegati dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, terroristico o comunque inappropriato o illegale;

b) prestare la massima attenzione nell'inoltro di e-mail riportanti contenuti e indirizzi e-mail di precedenti comunicazioni;

c) prestare la massima attenzione ad e-mail sospette, avvisando l'Amministratore di Sistema in caso di dubbi sulla provenienza/contenuto delle stesse;

d) creare una sezione denominata "Posta personale" all'interno della propria casella di posta, alla quale gli Amministratori di Sistema non potranno accedere se non per gravi motivi di sicurezza informatica.

Per motivi di sicurezza informatica ed in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'accesso alla casella di posta dell'Utente potrà essere gestito dagli Amministratori di Sistema su richiesta del Responsabile del Trattamento dell'Utente al fine di verificare il contenuto dei messaggi e dar seguito a quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

La **Posta Elettronica Certificata (PEC)** può essere utilizzata dagli Incaricati solamente per motivi professionali.

Articolo 23 - Utilizzo della navigazione internet

L'accesso a Internet è fornito principalmente per scopi professionali, per accedere a informazioni e contenuti necessari allo svolgimento dell'attività lavorativa. Essendo uno strumento di lavoro, gli Utenti cui si attribuisce l'accesso, sono responsabili del suo corretto utilizzo. Come per la posta elettronica, la Provincia di Ancona ne autorizza un moderato e ragionevole utilizzo privato, limitato ed ispirato a criteri di buon senso senza ostacoli all'attività professionale.

Il numero e la durata degli accessi a Internet sono costantemente registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge e dal mancato rispetto del presente Regolamento. Gli eventuali controlli compiuti dagli Amministratori di Sistema potranno avvenire mediante un sistema di analisi dei file giornale. Gli Utenti devono seguire le seguenti regole di navigazione della rete Internet:

a) è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da copyright, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all'interno della Provincia di Ancona;

b) è tassativamente vietato navigare siti e scaricare materiale pericolosi/vietati o aventi contenuti illegali (contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terrorismo o comunque inappropriato o illegale), salvo specifiche esigenze di ricerca;

c) è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso ma non limitato a digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;

d) è vietato utilizzare l'infrastruttura tecnologica della Provincia di Ancona per procurarsi e diffondere materiale in violazione con le normative vigenti;

e) è vietato effettuare attività che possano generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete;

f) è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all' host dell'Utente (sniffing) a meno che questa attività non faccia parte dei compiti dell'Utente e quindi formalmente autorizzata dagli amministratori di sistema;

g) è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete, account.

Articolo 24 - Filtro automatico alla navigazione internet

La Provincia di Ancona è dotata di un sistema di sicurezza perimetrale che permette di difendere e monitorare tutte le comunicazioni da e verso la rete internet (sistema UTM - Unified Threat Management – Sistema di gestione unificata delle minacce).

Grazie a questo sistema la Provincia di Ancona è in grado di ispezionare in maniera automatica e anonima il contenuto dei dati trasmessi e ricevuti e bloccarne il transito in base ad una serie di parametri. Uno di questi parametri è costituito dalla classificazione dei siti internet.

Al fine di evitare quanto più possibile controlli sulla navigazione degli Utenti, di evitare di essere coinvolto in attività illecite e di impedire, prima che avvengano, il verificarsi di pericoli o minacce al sistema telematico dell'Ente, la Provincia di Ancona impedisce la navigazione internet verso alcune tipologie di siti ritenuti in qualche modo pericolosi; il dettaglio relativo a questo filtro è presente nell'Appendice A al presente regolamento, che ne costituisce parte integrante.

Articolo 25 - Accesso internet per utenti esterni

Il sistema consente l'accesso e la navigazione in Internet ad Utenti esterni , ai sensi di quanto previsto dall'art 8-bis del D.Lgs 82/2005.

Articolo 26 - Accesso da remoto - virtual private network (vpn)

L'accesso dall'esterno alla rete della Provincia di Ancona è consentito esclusivamente attraverso precise modalità di connessione sicura.

Articolo 27 -Comunicazione di dati e informazioni attraverso social media

È assolutamente vietato pubblicare in internet attraverso social media personali, forum, chat, blog, siti internet, dati ed informazioni di carattere aziendale (informazioni, documenti, appunti, commenti personali o di terzi, foto, video, audio, ecc..) che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del know-how ed alla redditività della Provincia di Ancona o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.

È assolutamente vietato divulgare notizie false.

È invece autorizzata la divulgazione di informazioni già rese pubbliche dalla Provincia di Ancona.

Articolo 28 -Sistemi di monitoraggio rete aziendale

Per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare, per il tramite degli Amministratori di Sistema e nel rispetto della normativa sulla privacy, accedere direttamente a tutti gli strumenti informatici della Provincia di Ancona.

Periodicamente e in presenza di anomalie, gli Amministratori di Sistema effettueranno verifiche di funzionalità approfondite che potranno determinare segnalazioni ed avvisi generalizzati diretti agli Utenti della funzione organizzativa in cui è stata rilevata l'anomalia stessa e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

Gli Amministratori di Sistema effettuano inoltre forme di controllo di carattere impersonale sulla rete e su tutti i dispositivi che la compongono. I dettagli relativi ai controlli effettuati sono disponibili nell'Appendice B.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

LA Provincia di Ancona è tenuta comunque a denunciare all'autorità giudiziaria tutti i comportamenti contrari alla legge, anche rilevati da analisi di tipo impersonale.

Articolo 29 - Utilizzo della firma digitale

La Firma Digitale deve essere utilizzata esclusivamente dal proprietario della firma. Egli è responsabile della conservazione del dispositivo di firma e delle credenziali riservate per effettuare la firma. Anche qualora il titolare della firma volontariamente acconsentisse a far utilizzare la firma ad altri e ne dimostrasse l'utilizzo, tutti di documenti firmati digitalmente saranno considerati in ogni caso firmati dal titolare della firma il quale se ne assume ogni responsabilità.

Articolo 30 - Specifici divieti

Di seguito sono riportati specifici divieti per gli Utenti:

a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;

c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;

d) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico o di soggetti concorrenti, pubblici o privati al fine di acquisire informazioni riservate;

e) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

f) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;

g) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

h) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

i) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;

j) caricare programmi non provenienti da una fonte certa e autorizzata dall'Ente;

k) acquistare licenze software da una fonte (rivenditore o altro) non certificata e non in grado di fornire garanzie in merito all'originalità/autenticità del software, dietro parere favorevole dell'area Informatica e Telematica;

l) detenere supporti di memorizzazione di programmi non originali (DVD\CD\floppy);

m) installare un numero di copie di ciascun programma ottenuto in licenza superiore alle copie autorizzate dalla licenza stessa, al fine di evitare di ricadere in possibili situazioni di *underlicensing*;

n) utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;

o) utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;

p) distribuire il software istituzionale a soggetti terzi;

q) realizzare codice software che violi copyright di terzi;

r) accedere illegalmente e duplicare banche dati.

Articolo 31 - Perdita della qualifica di utente

In caso di cessazione del rapporto con la Provincia di Ancona, valgono le seguenti regole operative:

a) Le credenziali per l'accesso ai sistemi e alla posta elettronica vengono disattivate.

b) È facoltà della Provincia di Ancona effettuare eventuali operazioni di conservazione di e-mail di carattere professionale di Utenti non più appartenenti all'organizzazione. Le e-mail nella "Posta personale" saranno, al contrario, cancellate.

Tali attività sono effettuate dagli Amministratori di Sistema autorizzati alla gestione della posta elettronica, che potranno pertanto avere accesso, per esclusive ragioni di carattere tecnico e solo ove non sia evitabile, a dati personali conservati all'interno delle caselle di posta.

Con il dovuto anticipo, l'Utente è tenuto ad attivare il risponditore automatico per notificare ad eventuali fornitori, partner, clienti od altri soggetti interessati, l'interruzione del proprio rapporto con la Provincia di Ancona e - se del caso - per proporre un contatto interno alternativo.

Per quanto riguarda la restituzione degli strumenti informatici di proprietà della Provincia di Ancona, valgono le seguenti regole operative:

a) Gli smartphone e gli strumenti informatici affidati agli Utenti devono essere restituiti al Responsabile di Trattamento che li ha forniti.

Articolo 32 - Prescrizione residuale

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati e delle informazioni personali e aziendali, nonché sulle modalità di utilizzo degli strumenti di trattamento, l'Utente può rivolgersi al proprio Responsabile e al Responsabile della Prevenzione della Corruzione e Trasparenza (RPCT) e al Responsabile della Protezione dei Dati (RPD) per ricevere le opportune istruzioni.

Capo V - Responsabilità e sanzioni

Articolo 33 - Responsabilità e sanzioni

È fatto obbligo a tutti gli Utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione del presente Regolamento sono perseguibili nei confronti dell'Utente con provvedimenti disciplinari e risarcitori previsti dal vigente Codice Disciplinare della Provincia di Ancona, nonché con tutte le azioni civili e penali consentite.

Chiunque non rispetti il presente Regolamento potrà essere soggetto all'immediata sospensione dell'accesso agli strumenti informatici.

Capo VI - Aggiornamento e revisione

Articolo 34 - Aggiornamento e revisione

Il presente Regolamento è soggetto a revisione periodica, che potrà avvenire a seguito di cambiamenti organizzativi e normativi o necessità istituzionali. Tutte le future modifiche al presente Regolamento verranno opportunamente comunicate agli Utenti e rese pubbliche sul sito internet della Provincia di Ancona.

Letto ed approvato il _____

Appendice A

SISTEMA UTM (UNIFY THREAT MANAGEMENT):

La Provincia di Ancona non conserva i log di navigazione ma utilizza sistemi certificati che bloccano all'origine qualsiasi accesso verso siti censiti come malevoli o non afferenti alle attività dell'Ente. A titolo di esempio si riporta uno schema che illustra i primi dieci siti bloccati dall'UTM:

Categoria	Operazione
1.violance/hate/racism (violenza/odio/razzismo)	Block
2.intimate apparel/swimsuit (abbigliamento intimo, costumi da bagno)	Block
3.nudism (nudismo)	Block
4.pornography (pornografia)	Block
5.weapons (armi)	Block
6.adult/mature content (contenuti per adulti)	Block
7.drugs/illegal drugs (droghe/farmaci illegali)	Block

Appendice A

9. illegal skills/questionable skills (abilità illegali o discutibili)	Block
10. sex education (educazione sessuale)	Block
11. gambling (gioco d'azzardo)	Block
12. alcohol/tobacco (alcol/tabacco)	Block
13. Malware	Block

Appendice B

DETTAGLI RELATIVI ALLE ATTIVITÀ DI CONTROLLO SVOLTE DAGLI AMMINISTRATORI DI SISTEMA

La Provincia di Ancona gestisce i sistemi informatici e le reti anche attraverso strumenti che possono memorizzare temporaneamente e solo per esigenze di diagnosi o tuning dei sistemi i dati relativi alla navigazione internet e al traffico telematico. In particolare si elencano:

a) Posta Elettronica - dati conservati:

   1) log del traffico SMTP generato dai server di posta elettronica;

   2) log dei messaggi non correttamente inoltrati (ritardi e/o mancate consegne);

   3) log dei messaggi intercettati dal sistema antivirus.

b) Traffico IP – corretto funzionamento del sistema, monitoraggio SLA, controlli di sicurezza:

c) Log del traffico IP generato dai dispositivi informatici. Tale log comprende anche dati puntuali di navigazione riferibili all'indirizzo IP interno di provenienza della richiesta. Il log del traffico IP è memorizzato su un supporto volatile. Viene automaticamente cancellato al riavvio dell'apparato e gestito in modalità FIFO (first in first out) con un periodo di memorizzazione volatile massima non superiore alle tre giornate.

d) Telefonia – corretto funzionamento del sistema:

   1) Log delle chiamate (numero chiamante, numero chiamato, durata).

e) Accesso alle reti - corretto funzionamento del sistema e controlli di sicurezza:

   1) Log di accesso alle reti dall'esterno e dall'interno, sempre in modalità volatile.

Come indicato nelle Linee Guida del Garante per posta elettronica e internet, la Provincia di Ancona non procederà in nessun caso a controlli non consentiti, quali:

a) lettura e registrazione puntuale di messaggi di posta;

b) riproduzione e memorizzazione delle pagine internet visitate;

c) cattura dei caratteri digitati attraverso tastiera (fisica o virtuale);

d) analisi occulta dei pc affidati in uso.