REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI DI TE.AM. TERAMO AMBIENTE S.p.A.

Sommario

1 Riferimenti Normativi e documentali

1.1 Normativa europea

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("Regolamento Generale sulla Protezione dei Dati personali" o "GDPR").

1.1.1 Principi applicabili al trattamento di dati personali (Art 5, par. 1, del GDPR)

a) Liceità correttezza e trasparenza: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
b) Limitazione della finalità: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.
c) Minimizzazione dei dati: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
d) Esattezza: i dati personali sono esatti e, se necessario, aggiornati; devono essere adottate tutte le
e) misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
f) Limitazione della conservazione: i dati personali sono conservati in una forma che consenta
g) l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
h) Integrità e riservatezza: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

1.1.2 Sicurezza del trattamento (Art. 32, par. 1 del GDPR)

- Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il Responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

1.2 Normativa italiana

a) Decreto Legislativo 30 giugno 2003, n. 196, come modificato dal D.Lgs. 101/2018 e successive integrazioni e modificazioni ("Codice in materia di protezione dei dati personali").

b) Legge 20 maggio 1970, n. 300 e successive integrazioni e modificazioni, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento" ("Statuto dei Lavoratori").

c) Decreto Legislativo 8 giugno 2001, n. 231, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle Aziende e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300", pubblicato in Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni e integrazioni.

d) Articolo 23 del Decreto Legislativo n. 151/2015 (c.d. Jobs Act) integrante il divieto dei controlli a

e) distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

f) Decreto Legislativo 29 dicembre 1992 n. 518 Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore.

g) Legge 22 aprile 1941 n. 633 s.m.i. sulla tutela del diritto d'autore.

h) Legge 13.12.1993 n. 547 (Modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica)

i) Legge 18 agosto 2000 n. 248 s.m.i. (Tutela del diritto di autore).

j) DPR nr. 81 del 13.06.2023 che modifica il codice di comportamento dei dipendenti pubblici (DPR n. 62 del 16.04.2013).

k) Codice civile:

- Art. 2049: Responsabilità indiretta dell'imprenditore;
- Art. 2086: Direzione e gerarchia nell'impresa;
- Art. 2087: Tutela dell'integrità fisica e della personalità morale dei dipendenti, da parte dell'imprenditore;
- Art. 2104: Diligenza del dipendente nel rispetto delle disposizioni impartite dall'imprenditore.

1.3 Provvedimenti Autorità garante per la protezione dei dati personali

a) Linee Guida del Garante Privacy su Posta Elettronica e Internet (doc. web n. 1387522 – Deliberazione n. 13 del 1° marzo 2007 – G.U. n. 58 del 10 marzo 2007);
b) Provvedimento relativo al "Trattamento di dati personali effettuato sugli account di posta elettronica
c) aziendale" - 1° febbraio 2018" n. 53 (doc. web n.8159221)
d) Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008(G.U. n. 300 del 24 dicembre 2008) doc. web n. 1577499.

1.4 Agenzia per l'italia digitale - Agid

- Circolare dell'Agenzia per l'Italia Digitale – AGID n. 2 del 18 aprile 2017 relativo a "Misure minime di sicurezza ICT per le pubbliche amministrazioni".

2 Definizioni

a) *Amministratore di Sistema*: con Amministratore di Sistema (AdS) si individuano, generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente regolamento vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;
b) *Apps*: Applicazioni che possono essere rese disponibili / scaricate da diverse fonti, quali app-store on-line correlati a piattaforme dei produttori dei dispositivi, siti pubblici online non correlati a specifici produttori, elenchi di applicazioni sviluppate in ambito aziendale;
c) *Autenticazione*: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso;
d) *Banca di dati o 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;
e) *Blocco*: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

f) *BYOD* (Bring Your Own Device): approccio per l'utilizzo dei dispositivi mobili evoluti in ambito aziendale che prevede che gli utenti dei servizi informativi aziendali possano utilizzare il dispositivo di loro proprietà;

g) *Comunicazione*: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

h) *Comunicazione elettronica*: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

i) *Credenziali di autenticazione*: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

j) *Diffusione*: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

k) *Dato anonimo*: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

l) *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;

m) *Dato a conoscibilità limitata*: il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti;

n) *Dato delle pubbliche amministrazioni*: il dato formato, o comunque trattato da una pubblica amministrazione;

o) *Dato pubblico*: il dato conoscibile da chiunque;

p) *Dati identificativi*: i dati personali che permettono l'identificazione diretta dell'interessato;

q) *Dati particolari*: 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;

r) *Dati giudiziari*: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di

anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

s) *Disponibilità*: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di Legge;

t) *Documento informatico*: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

u) *Jailbreaking*: attività effettuata su un dispositivo (generalmente contro le regole/politiche che ne determinano l'utilizzo) al fine di permettere un'estensione dei servizi disponibili;

v) *Incaricati al trattamento*: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

w) *Interessato*: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

x) *Firma elettronica*: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;

y) *Firma digitale*: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

z) *Fruibilità di un dato*: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;

aa) *Garante*: l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675;

bb) *Gestione informatica dei documenti*: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;

cc) *Parola chiave o Password:* componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

dd) *Posta elettronica*: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza;

ee) *Posta Elettronica Certificata* (PEC): sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;

ff) *Profilo di autorizzazione*: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

gg) *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;

hh) *Reti di comunicazione elettronica*: i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

ii) *Strumenti elettronici*: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

jj) *Sistema di autorizzazione*: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;

kk) *Smartphone*: uno smartphone è un dispositivo portatile, alimentato a batteria, che coniuga le funzionalità di telefono cellulare con quelle di elaborazione e trasmissione dati tipiche del mondo dei personal computer;

ll) *Tablet*: dispositivi assimilabili per componenti hardware e software agli smartphone, dai quali si distinguono per dimensioni dello schermo, possibile assenza del modulo telefonico, assenza di funzioni telefoniche;

mm) *Titolare del trattamento*: a 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;

nn) *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;

oo) *Validazione temporale*: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;

pp) *Violazione dei dati personali*: la 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;

qq) *VPN* (Virtual Private Network): modalità di trasmissione dati in modalità privata (criptata o analogo) su rete pubblica, tipicamente Internet.

3 Oggetto e ambito di applicazione

1. Con il presente Regolamento sono disciplinate le condizioni di utilizzo delle risorse informatiche che la Team Teramo Ambiente S.p.a. (di seguito anche "Te.Am.") mette a disposizione del personale dipendente e non dipendente per l'esecuzione dei propri compiti lavorativi di competenza, al fine di tutelare il patrimonio informativo dello stesso.
2. In tal senso la Rete di Te.Am. è costituita dall'insieme delle risorse infrastrutturali e dal patrimonio informativo digitale posseduto o gestito dalla Società. Per Risorse Infrastrutturali si intendono i componenti hardware e software. Il Patrimonio Informativo, invece, è l'insieme delle Banche Dati in formato digitale e, in generale, tutti i documenti prodotti tramite l'utilizzo degli strumenti appartenenti alla infrastruttura ICT.
3. Il presente Regolamento si applica a tutti gli utenti interni ed esterni che sono autorizzati ad accedere alla Rete Aziendale o ad utilizzare sistemi elaborativi di Te.Am.. Per utenti interni si intendono tutti gli Amministratori, i Dirigenti, i dipendenti a tempo indeterminato e a tempo determinato e i collaboratori anche occasionali.

4 Ruoli e responsabilità

4.1 ICT (Information and Communication Technologies) – Area Tecnica e Servizi

1. ICT è Responsabile della definizione degli aspetti di sicurezza tecnico-organizzativi inerenti ai servizi informatici della TEAM e, quindi, definisce, in applicazione dei principi guida e le linee di indirizzo che riceve dal CdA, le procedure organizzative e/o operative che regolamentano i servizi informatici della Te.Am.
2. In particolare, ICT è Responsabile di definire:
   - le politiche di URL Filtering, identificando le categorie di siti Internet il cui accesso sarà bloccato in quanto contrari alla legge, all'ordine pubblico, al buon costume, all'etica della TEAM, nonché di contenuto oltraggioso o discriminatorio;
   - di analizzare, in forma aggregata ed anonima, i log di sicurezza e di individuare le possibili contromisure per risolvere eventuali minacce alla sicurezza;

- di stabilire il limite massimo dello spazio riservato alle caselle di posta elettronica sul server e le dimensioni massime consentite per i messaggi inviati e ricevuti;
- di provvedere all'attività di installazione ed attivazione di software antivirus o di analisi di comportamenti anomali a protezione delle Postazioni di lavoro degli utenti;
- di definire i processi di creazione, abilitazione, modifica, disattivazione, ripristino e cessazione degli account di accesso ai servizi informatici, dietro esplicita e specifica richiesta pervenuta dai competenti Uffici;
- proporre al CdA modifiche al Regolamento in caso di variazioni normative e/o relative all'organizzazione della TeAm.;
- al fine di garantire la corretta attuazione del presente Regolamento, porre in essere tutte le misure operative e proporre al CdA l'adozione di eventuali procedure ritenute necessarie;
- notificare al CdA eventuali violazioni del Regolamento.

3. ICT è il punto di contatto per la gestione degli incidenti informatici e, più in generale, degli utilizzi non corretti degli strumenti correlati e delle violazioni informatiche, fermo restando il rispetto di quanto previsto dalla "Procedura per la gestione e la notifica del data breach" vigente (PSI-GDPR-DB Rev. 1 del 03/09/2019).

4.2 Responsabili di Area, di Ufficio, Referenti privacy

1. Sono tenuti alla distribuzione, sensibilizzazione e verifica dell'applicazione del presente Regolamento.
2. È responsabilità dei Responsabili di Area, di Ufficio, Referenti Privacy, nei cui ambiti sono previsti accessi ai sistemi informatici e/o telefonici della TeAm, di notificare a tutti i soggetti interessati il presente Regolamento (incaricati al trattamento), di farlo adottare nonché di sovrintendere alla sua corretta applicazione.

4.3 Dipendenti

1. I dipendenti della TeAm e, in generale, a tutti coloro che, in virtù di un rapporto di lavoro o fornitura (per esempio, consulenti, fornitori, stagisti, risorse in somministrazione di seguito denominati utenti esterni), gestiscono ed utilizzano gli strumenti informatici forniti dall'azienda sono personalmente responsabili in particolare, oltre che della piena osservanza del presente Regolamento:
   - delle credenziali a loro assegnate, sia per la loro generazione in conformità con le indicazioni di ICT che della loro custodia e non divulgazione;

- di tutte le attività che svolgono attraverso l'utilizzo degli strumenti informatici e/o telefonici;
- della pronta comunicazione di difformità da parte propria o dei colleghi rispetto a quanto previsto dal presente Regolamento;
- della massima attenzione a tutti i temi di Sicurezza Informatica qui indicati e/o comunicati in itinere da ICT.

4.4 Utenti esterni

1. Per utenti Esterni si intendono: le ditte fornitrici di software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, enti esterni autorizzati da collaboratori esterni e consulenti autorizzati.

5 Principi generali

1. Te.Am. Teramo Ambiente S.p.a. promuove l'utilizzo degli strumenti propri delle Tecnologie dell'Informazione e della Comunicazione (ICT) per il perseguimento delle proprie finalità e della "Mission" aziendale.
2. Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei valori e degli obiettivi della Azienda, dei diritti degli altri utenti e di terzi, salvaguardando l'integrità dei sistemi e delle relative risorse, in osservanza di Leggi, norme e obblighi contrattuali.
3. Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina oltre che di legalità. Ogni utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche, dei servizi applicativi e dei programmi ai quali ha accesso nonché dei propri dati.
4. La postazione di lavoro costituita da Personal Computer, periferiche, software di base, software applicativi e connessione alla rete, viene consegnata completa di quanto necessario per svolgere le proprie funzioni; pertanto è vietato modificarne la configurazione senza la previa autorizzazione dell'Amministratore di Sistema.
5. Il software applicativo installato sui Personal Computer è quello necessario all'espletamento dalle specifiche attività lavorative dell'operatore. E, pertanto, fatto divieto di installare qualsiasi programma da parte dell'utente o di altri operatori senza il previo consenso dell'Amministratore di Sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza. A riguardo l'Amministratore di Sistema ha facoltà di procedere a verifiche e controlli.

6. Ogni utente è responsabile dei dati memorizzati nel proprio Personal Computer compresi eventuali supporti rimovibili. Per questo motivo egli è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato, sentito l'Amministratore di Sistema.
7. Per ragioni di sicurezza e protezione dei dati e dei sistemi, le attività compiute nella Rete Informatica possono essere soggette a rilevamento e registrazione in appositi file (log) e ed essere ricondotte ad uno specifico account di rete. Tali file, tuttavia, possono essere soggetti a trattamento esclusivamente per fini istituzionali, per attività di monitoraggio e controllo e possono essere messi a disposizione dell'Autorità Giudiziaria in caso di accertata violazione della Normativa vigente. La riservatezza delle informazioni in essi contenute è garantita in base alla normativa vigente.

6 Soggetti legittimati all'utilizzo degli strumenti ICT

1. L'utilizzo della Posta Elettronica e l'accesso ad Internet sono accordati al dipendente con lettera di designazione ad "incaricato del trattamento".
2. Il Titolare del Trattamento designa uno o più "Responsabili", fornendo loro precise istruzioni sui tipi di controllo ammessi e sulle relative modalità.
3. Agli incaricati alla amministrazione e/manutenzione dei sistemi ICT è vietato l'accesso ai dati personali presenti in cartelle o spazi di memoria eventualmente assegnati ai dipendenti, ed è posto l'obbligo di svolgere esclusivamente le operazioni strettamente necessarie per adempiere al proprio incarico. Ai dipendenti sono resi noti i compiti ed i nominativi dei manutentori.
4. L'Amministratore di Sistema può compiere le operazioni strettamente necessarie per adempiere al proprio incarico come da provvedimento del Garante della Privacy in materia.

7 Divieti di utilizzo degli strumenti informatici

1. Al fine di garantire la funzionalità, la sicurezza ed il corretto impiego degli strumenti elettronici e, al tempo stesso, la protezione della riservatezza dei dipendenti, messa a rischio dalla possibilità di costante monitoraggio offerte dalla tecnologia (es.: profilazioni, comunicazione/diffusione di dati personali, anche sensibili), vengono esplicitate le seguenti limitazioni relative all'utilizzo e alle modalità di impiego delle risorse ICT aziendali.

7.1 Divieto di utilizzo di Personal Computer

Sono vietati:

1. L'accesso al Sistema Informatico ed il mantenersi all'interno di essi per motivi non lavorativi o non di servizio al di fuori della fascia oraria compresa dalle ore 14:00 alle ore 15:00, dal lunedì al sabato, intervallo nel quale TEAM consente al personale in servizio l'utilizzo degli strumenti informatici forniti (i.e. Personal Computer e accesso Internet) per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, ferma restando la liceità della condotta. Eventuali documenti di natura personale dovranno essere rimossi senza indugio.
2. L'installazione di programmi personali ulteriori rispetto a quelli forniti da TEAM.
3. La modificazione delle configurazioni impostate dall'Amministratore di Sistema.
4. L'utilizzo di supporti di memoria (es. Dischi esterni o pendrive USB) senza preventiva autorizzazione del Titolare, sentito l'Amministratore di Sistema.

8 Divieto di utilizzo della rete Internet

Premesso che l'azienda adotta un servizio di filtraggio della navigazione Web, non è consentito:

1. Navigare su siti Web non correlati con la prestazione lavorativa al di fuori dell'intervallo concesso di cui all'art. precedente;
2. Il download di programmi o di file multimediali (audio, video, etc.), salvo espressa autorizzazione da parte dell'Amministratore di Sistema;
3. La partecipazione a forum, Social network, chat, aste online e la fruizione di servizi di e-commerce senza autorizzazione del Titolare del Trattamento, sentito l'Amministratore di Sistema.
4. La acquisizione, archiviazione, conservazione, trasmissione di file a contenuto offensivo, discriminatorio, illecito penalmente e civilmente;
5. L'utilizzo per finalità ludiche.

9 Divieti di utilizzo della Posta Elettronica

Non è consentito:

1. L'uso della Posta Elettronica aziendale per ragioni non attinenti ai compiti affidati e alla mansione.
2. L'invio o la archiviazione di messaggi offensivi o discriminatori.
3. L'uso della Posta Elettronica "semplice" ossia senza l'integrazione di funzioni di sicurezza quali crittografia e protezione degli allegati con password, per documenti riservati e confidenziali.
4. L'uso della Posta Elettronica per partecipare a dibattiti, forum o mailing list non pertinenti all'attività lavorativa o, comunque, di contenuto offensivo o discriminatorio.

5. L'invio di messaggi di posta elettronica, all'interno o all'esterno dell'Azienda, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'Azienda stessa.

10 Prevenzione dell'utilizzo improprio

1. Gli strumenti informatici, intesi in senso lato, sono di proprietà della Azienda e devono essere utilizzati per fini produttivi e professionali. A ciascun dipendente viene demandata la responsabilità di utilizzare la infrastruttura e le attrezzature (Personal Computer, cellulari, notebook, rete, etc.) nonché gli accessori ad esse connessi, in modo professionale, lecito e sicuro, rispettando le Leggi vigenti, i comuni principi morali ed etici, la privacy e la riservatezza dei dati trattati.
2. Ciascun dipendente è responsabile per l'utilizzo, in violazione del presente regolamento, da parte di terzi, anche se conosciuti o affini, del computer aziendale e, in generale, degli strumenti a lui eventualmente affidati.
3. Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'amministrazione di appartenenza. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

11 Utilizzo degli strumenti ICT alla conduzione di automezzi

- E' fatto divieto di utilizzo degli strumenti informatici, in particolare quelli "mobili" come smartphone, palmari e tablet, ancorché per finalità lavorative, mentre si è alla conduzione di automezzi o mentre si utilizzano attrezzature di lavoro (es. gru, trattori, decespugliatori, scale, etc.);
- Il divieto si applica parimenti agli strumenti ICT in dotazione per specifiche applicazioni di servizio (es. palmari o tablet per identificazione utenza o contenitori);
- E', in ogni caso, vietato l'utilizzo degli strumenti informatici nei modi e nelle condizioni interdette da Norme sovraordinate anche se non esplicitamente indicato nel presente Regolamento.

12 Utilizzo dei mezzi di informazione e dei social media

1. Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente all'Azienda di appartenenza.

2. In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.
3. Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.
4. Fermi restando i casi di divieto previsti dalla Legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'amministrazione e in difformità alle disposizioni di cui al Decreto Legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.

13 Internet

1. Tutti i dipendenti sono tenuti a utilizzare i servizi di rete esclusivamente nell'ambito delle proprie mansioni di lavoro, secondo direttive circostanziate nella consapevolezza che ogni accesso ad una risorsa può essere facilmente ricondotto alla persona che lo ha effettuato.
2. Tutti i dipendenti devono agire con il massimo livello di professionalità quando operano in Internet evitando di catalizzare o provocare eventi dannosi anche al fine di non ledere l'immagine dell'Azienda.
3. Vengono, in ogni caso, messe in atto tutte le necessarie precauzioni al fine di evitare che intrusi possano intromettersi, attraverso Internet, nel sistema informatico aziendale (firewall perimetrale) o che attraverso Internet possano essere introdotti virus o altre forme di malware (antimalware centralizzato);
4. E' fatto divieto di abbandonare la propria postazione informatica propria postazione informatica lasciando aperta la sessione di lavoro.
5. La connessione Internet deve essere utilizzata per gli scopi ed il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento fatta eccezione per quanto stabilito al paragrafo 7.1.
6. Vengono individuate congiuntamente dal Titolare del Trattamento e dall'Amministratore di Sistema, sentiti i Responsabili degli Uffici, le categorie dei siti web considerate necessarie o correlate con la prestazione lavorativa, con conseguente configurazione del sistema di filtraggio Web in modo da interdire l'accesso ai siti non correlati.

7. Vengono adottati sistemi di filtraggio finalizzati a prevenire la esecuzione di determinate operazioni reputate non attinenti all'attività lavorativa, quali l'upload o l'accesso a determinati siti e/o il download e l'esecuzione di file o software aventi particolari caratteristiche (dimensionali o tipologiche).
8. E' vietato fornire a terzi l'accesso alla connessione Internet aziendale senza la esplicita autorizzazione dell'Amministratore di Sistema.
9. E' vietato prestare o cedere a terzi qualsiasi apparecchiatura informatica aziendale.
10. Non sono consentiti, salvo specifica ed esplicita autorizzazione dell'Amministratore di Sistema, impieghi di applicazioni cosiddette "portabili", ossia eseguibili direttamente da memorie esterne (es. Winpenpack, PortableApps, etc.).

14 Posta Elettronica

1. La Posta elettronica aziendale è uno strumento di lavoro ed in quanto tale resta di esclusiva proprietà della Azienda e deve essere utilizzato esclusivamente per fini professionali in riferimento alle specifiche mansioni attribuite all'utente in ambito aziendale.
2. L'uso della Posta Elettronica Aziendale comporta, da parte dell'utente, l'impegno e la esposizione contestuale del marchio, dell'immagine e dei valori dell'Azienda e, di conseguenza, costituisce una assunzione di responsabilità in tal senso: quando si utilizza la casella di Posta Elettronica Aziendale per comunicare, si rappresenta l'Azienda verso terzi;
3. Non è ammesso l'utilizzo per fini esclusivamente personali della posta elettronica aziendale in uscita;
4. L'utilizzo della casella di posta aziendale in entrata per fini personali è ammesso esclusivamente in via occasionale e non interferente con l'attività lavorativa, nel pieno rispetto delle misure di sicurezza (fisiche, logiche e procedurali) adottate, per contenuti legali, consoni e appropriati. L'utente assume la piena responsabilità dei contenuti che dovesse ricevere nella casella di posta aziendale.
5. Gli accessi alle caselle di posta elettronica devono essere sempre riconducibili ad una persona fisica e, pertanto, ciascun utente deve accedere alla casella email assegnatagli utilizzando in forma esclusiva le proprie credenziali di autenticazione;
6. Sono resi disponibili, in deroga circostanziata al comma precedente, indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@teramoambiente.it, ufficioacquisti@teramoambiente.it, segreteriapresidenza@teramoambiente.it etc.), affiancati a quelli individuali con la convenzione <iniziale_nome>.<cognome>@teramoambiente.it.

7. In calce ad ogni email, inseriti come firma, devono essere riportati i dati di recapito del mittente, la funzione aziendale, il logo aziendale e la dichiarazione relativa alla riservatezza dei contenuti comprensiva di avvertimento per i destinatari sulla natura non personale dei contenuti e del fatto che le risposte possono essere conosciute dall'Azienda (conformemente a quanto rappresentato nell'allegato 1).
8. In caso di assenze non programmate (malattia, etc.) che si protraggono per più di 15 (quindici) giorni lavorativi, il Titolare del Trattamento provvederà, qualora necessario, mediante personale appositamente incaricato (es. Amministratore di Sistema) al ripristino della password della casella di posta della persona non disponibile onde accederne ai contenuti. Al rientro dell'interessato verrà riattivata la procedura di rilascio della password esclusiva.
9. In caso di assenza improvvisa o prolungata, se improrogabili necessità di lavoro richiedono la conoscenza dei messaggi di posta elettronica, il Titolare del Trattamento, informato preliminarmente l'interessato affinché possa rimuovere eventuali contenuti personali, ha facoltà di delegare un altro incaricato alla verifica del contenuto dei messaggi di posta elettronica.
10. Per quanto ogni server aziendale sia dotato di idonei strumenti di protezione, resta in capo agli utenti la responsabilità della adozione di comportamenti responsabili e di un atteggiamento consapevole verso i rischi derivanti dall'utilizzo di posta elettronica (malware, phishing, vishing, smishing, spamming).
11. In relazione al disposto del comma precedente, è fatto divieto, agli utilizzatori di posta elettronica di aprire file allegati a messaggi email la cui provenienza risulti incerta o sospetta così come di cliccare su link la cui provenienza non sia definitamente nota e concordata.
12. Qualora un utente avesse ragione di sospettare la avvenuta introduzione, nel proprio sistema, di codice maligno, è tenuto a scollegare immediatamente senza alcun indugio il cavo di rete e ad avvisare l'Amministratore di Sistema.
13. Non è consentito l'utilizzo del sistema di posta elettronica in forme che possano tradursi in un danno o semplicemente un disturbo oggettivo arrecato a terzi.
14. E fatto divieto di consentire a terzi l'accesso e/o l'utilizzo del servizio di posta elettronica aziendale.
15. E fatto divieto a qualsiasi utente del servizio di posta elettronica di alterare il contenuto delle intestazioni (headers) dei protocolli di comunicazione o di falsificare l'indirizzo email del mittente (spoofing).
16. L'accesso dall'esterno alla propria casella email aziendale è consentito esclusivamente attraverso l'appropriato servizio webmail (www.teramoambiente.it/webmail).

15 Utilizzo della LAN e della Intranet

1. Le unità di rete (dischi condivisi, NAS, SAN, file server, etc.) sono aree di condivisione di informazioni strettamente professionali e a carattere riservato: in quanto tali non possono in alcun modo essere utilizzate per scopi personali. In queste unità non è consentita la archiviazione di files con contenuti diversi da quelli attinenti alle attività lavorative, neppure per brevi periodi o in via occasionale.
2. Le unità di rete sono oggetto di regolari attività di controllo, amministrazione e salvataggio dati da parte dell'Amministratore di Sistema e/o dagli incaricati da questi individuati.
3. Le password di accesso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure definite e le istruzioni impartite. E' assolutamente vietato accedere ai sistemi e alle applicazioni con le credenziali di altri utenti. Tale condotta può integrare le fattispecie di accesso abusivo ad un sistema informatico (cfr. art. 615 ter del Codice Penale) e detenzione abusiva di codici di accesso ad un sistema informatico (art.615 quater del Codice Penale).
4. L'Amministratore del Sistema può, in qualunque momento e dandone comunicazione agli eventuali interessati, procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
5. I file generati dagli utenti (documenti, immagini, etc.) nell'espletamento della mansione devono essere salvati nelle apposite cartelle di rete indicate dall' Amministratore di sistema e, salvo diversa indicazione, non localmente (Desktop o cartella documenti) al Personal Computer in uso dall'utente stesso.
6. Le copie di sicurezza (backup) degli eventuali files di lavoro archiviati, in via eccezionale come da comma precedente, localmente al sistema di elaborazione in uso, sono in capo all' utente.
7. È in capo a ciascun utente la pulizia periodica, con cadenza almeno semestrale, dei propri archivi, con la rimozione di files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati onde evitare una archiviazione ridondante con sovrautilizzo delle risorse di storage e della banda passante per i backup.
8. Per ciò che riguarda le stampanti condivise, è cura dell'utente, dopo aver effettuato la stampa dei propri documenti, ritirarli tempestivamente dal vassoio della stampante.
9. Al fine di proteggere la riservatezza dei documenti stampati, ogni dipendente, allorquando si reca a ritirare le stampe, dovrà digitare un codice univoco che gli sarà fornito dalla TEAM, a seguito del quale la stampante multifunzione provvederà a far uscire i fogli stampati.
10. Poiché la banda della rete è una risorsa condivisa e limitata, ogni utente ha in capo la responsabilità di non compiere operazioni (upload o download di file multimediali, invio di mail con allegati molto

grandi, ascolto in streaming, etc.) che tendano a monopolizzare la banda passante a discapito degli altri legittimi utenti.

16 Utilizzo della postazione di lavoro

1. La Postazione di Lavoro (PdL), intesa come l'insieme di apparecchiature e dispositivi elettronici quali Personal Computer, Monitor, Stampante, Scanner, Videocamera, etc., è uno strumento di lavoro ed un utilizzo improprio comporta rischi elevati per la sicurezza aziendale. Qualsiasi utilizzo diverso da quello previsto nel presente regolamento non è consentito.
2. L'accesso ai sistemi di elaborazione è protetto da password, la quale deve essere custodita dall'incaricato con la massima diligenza e non divulgata o comunicata ad altri.
3. All'utente della PdC non è consentito modificare le configurazioni impostate senza l'esplicita autorizzazione dell'Amministratore di Sistema.
4. All'utente della PdC non è consentito installare autonomamente programmi e applicazioni senza l'esplicita autorizzazione dell'Amministratore di Sistema.
5. Non è consentito l'utilizzo di programmi o applicazioni diversi da quelli ufficialmente distribuiti dal Titolare del trattamento.
6. Non è consentito, se non previa esplicita autorizzazione dell'amministratore di sistema, installare sul Personal Computer aziendale periferiche hardware proprie o connettere le attrezzature ICT aziendali tra loro o con altri dispositivi (telefoni cellulari, palmari, etc.) di proprietà personale salvo quanto previsto dal presente regolamento in materia di BYOD.
7. L'Amministratore di Sistema, per l'espletamento delle sue funzioni ed esclusivamente in circostanze che ne giustifichino la necessità (data breach, business continuity, disaster recovery, minacce alla sicurezza, controlli difensivi) la facoltà di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica (cfr. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – 27 novembre 2008, pubblicato in G.U. n. 300 del 24 dicembre 2008, modificato con provvedimento del 25/06/2009);
8. Le apparecchiature costituenti la Postazione Di Lavoro devono essere spente prima di lasciare gli uffici o in caso di assenze prolungate dallo stesso. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo abusivo da parte di terzi.
9. L'istallazione nella PdL di dispositivi di memorizzazione o comunicazione (es. pendrive, telecamere, etc.) è consentita esclusivamente previa esplicita autorizzazione dell'Amministratore di Sistema.

10. È fatto divieto di accedere simultaneamente, con il medesimo account, da più postazioni di lavoro, salvo autorizzazione dell'Amministratore di Sistema.
11. È fatto obbligo a tutti gli utenti verificare i dati di origine esterna prima di ogni trattamento, avvertendo immediatamente e senza indugio nel caso in cui i sistemi di sicurezza segnalassero il rinvenimento di un malware.
12. Non è consentito il trattamento di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
13. È fatto obbligo, ogniqualvolta ci si allontana dalla postazione, di bloccare la sessione di lavoro (tasto WINDOWS+L) estraendo eventuale hardware di autenticazione (es. token).

17 Utilizzo di supporti di memorizzazione rimovibili

1. Non è consentito collegare, inserire o utilizzare supporti rimovibili personali se non dietro esplicita autorizzazione dell'amministratore di sistema: I supporti eventualmente autorizzati devono essere comunque sottoposti a scansione antimalware preventiva.
2. Non è consentito scaricare o comunque salvare i contenuti dei sistemi di elaborazione aziendale su supporti removibili senza autorizzazione sia del Titolare del trattamento sia dell'Amministratore di sistema.
3. I supporti rimovibili contenenti dati personali, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (cfr. Provvedimento a carattere generale del 13/10/2008). I supporti contenenti dati particolari devono essere custoditi in archivi chiusi a chiave.
4. Tutti i files di provenienza esterna o incerta, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e all'eventuale autorizzazione all'utilizzo, dell'Amministratore di Sistema e del competente Referente Privacy.

18 Utilizzo di sistemi di elaborazione portatili

1. L'utente è responsabile dei dispositivi e sistemi di elaborazione portatili (es. notebook, videoproiettore, etc.) assegnatogli o comunque utilizzati, ed è tenuto a custodirli con diligenza sia durante eventuali spostamenti o trasferimenti, sia nel corso del loro utilizzo.
2. Ai PC portatili si applicano le regole di utilizzo previste per le Postazioni Di Lavoro, con particolare attenzione alla rimozione di eventuali files elaborati sullo stesso prima della riconsegna.

3. I PC portatili esternamente all'azienda (convegni, sessioni formative, riunioni, etc.) devono essere costantemente custoditi e, in caso, di temporaneo allontanamento, protetti con misure fisiche (es. armadietto con serratura).

19 Utilizzo di dispositivi mobili

1. Non è ammesso, per ragioni di sicurezza, il collegamento alla rete LAN aziendale attraverso dispositivi di tipo "mobile" come smartphone o tablet.
2. È vietato l'utilizzo di "internet key" mobile cosi come di hotspot personali e tethering con i sistemi elaborativi aziendali.
3. Nel caso in cui il dispositivo venga utilizzato per svolgervi un qualsiasi trattamento di dati personali, è fatto obbligo all'utilizzatore, di attivare l'accesso con password, il blocco automatico del dispositivo, il tracciamento del dispositivo e la possibilità di cancellazione remota dei dati (modalità "furto").
4. Sono precluse operazioni tipo "jailbreaking" (dispositivi Apple) o "root" (dispositivi Android), su qualsiasi dispositivo o sistema aziendale.

20 BYOD (Bring Your Own Device)

1. È ammesso l'utilizzo di dispositivi personali per lo svolgimento della prestazione lavorativa esclusivamente alle seguenti condizioni:
   - Smartworking;
   - Situazioni specificamente autorizzate dal Titolare del Trattamento sentito l'Amministratore di Sistema.
2. In ogni caso, l'utente deve:
   - Consentire all'Amministratore di Sistema la verifica preliminare della compatibilità e della idoneità del proprio dispositivo rispetto alla infrastruttura e alle policy aziendali;
   - Consentire l'installazione dei programmi aziendali di contrasto e prevenzione al malware;
   - Consentire l'installazione dei programmi aziendali di manutenzione e assistenza remote;
   - Adottare tutte le misure relative allo PdL prescritte dal presente regolamento.
   - Evitare di archiviare in locale al dispositivo documenti e file a carattere aziendale contenenti dati personali;
   - Fornire copia dei dati trattati per conto del Titolare e, a sua richiesta e, comunque, al momento della cessazione di utilizzo BYOD del dispositivo, provvedere alla loro cancellazione.

3. E' precluso il ricorso al BYOD con dispositivi o sistemi sui quali siano stati attuati interventi di jailbreaking o root, o siano presenti programmi sprovvisti di regolare licenza di utilizzo o che comportino vulnerabilità per l'infrastruttura aziendale.
4. Il collegamento di dispositivi mobili (tablet e smartphone) non aziendali alla LAN non è consentito;
5. Il collegamento di laptop/notebook/netbook non aziendali (es. notebook personale, consulente, fornitore) alla LAN è deprecato ma consentito in casi residuali e motivati, alle seguenti condizioni:
    a. Il Dirigente/Responsabile dell'area avente oggettiva necessità ne dà preavviso al Titolare e all'Amministratore di Sistema specificando il tipo di attività e le banche dati aziendali interessate.
    b. Il detentore del dispositivo consente all'Amministratore di Sistema di verificare l'idoneità del dispositivo (assenza di malware, presenza di antimalware e firewall, sistema operativo adeguato e aggiornato, etc.).

21 Accesso alla rete da parte di utenti esterni

Si considerano utenti esterni, i soggetti senza un rapporto di lavoro subordinato con TEAM e sprovvisti di designazione a incaricato del trattamento

Affinché un utente esterno possa essere autorizzato all'uso delle risorse informatiche aziendali e dei relativi servizi, è necessario che disponga di un incarico formale e, se del caso e sentito RPD, di designazione a Responsabile del Trattamento ai sensi dell'art.28 del Regolamento UE 2016/679.

A seguito della richiesta scritta del Dirigente/Responsabile competente, l'Amministratore di Sistema provvederà alla creazione di un account per l'accesso ai sistemi aziendali con i privilegi minimi necessari allo svolgimento dell'attività.

22 Accesso dall'esterno

1. Non è, in generale, consentito accedere dall'esterno alla rete LAN aziendale ed alle sue risorse: le regole dei sistemi di elaborazione e degli apparati di comunicazione, saranno configurati in tal senso.
2. Eccezionalmente, è consentito l'accesso dall'esterno nelle condizioni di smartworking previste dalla normativa vigente
3. Qualora insorgesse la necessità di erogare servizi applicativi all'esterno della rete LAN, si dovrà implementare una apposita "DMZ" separata dalla rete "fidata" contenente le banche dati e i servizi

critici, ovvero si ricorrerà ad un servizio cloud (paradigma SaaS) con le idonee garanzie di affidabilità e sicurezza.

4. L'accesso dall'esterno ai sistemi interni è consentito esclusivamente all'Amministratore di Sistema e ai Manutentori incaricati, per finalità manutentive, tramite tunnel cifrato (VPN) con protocolli allo stato dell'arte e previo superamento di una procedura di autenticazione e autorizzazione.

23 Gestione delle credenziali

1. L'accesso alle risorse informatiche aziendali deve sempre essere protetto da password o con altra misura di autenticazione robusta (es. autenticazione a più fattori) ed il livello di accesso di ciascun utente disciplinato da un sistema di autorizzazione così come previsto dalle normative comunitarie e nazionali vigenti in tema di trattamento dei dati personali.
2. Le password di accesso ai sistemi di elaborazione, al software applicativo e alle risorse di rete, sono previste e attribuite in forma scritta dall'Amministratore di Sistema in riscontro alla richiesta di attivazione credenziali inoltrata, sempre in forma scritta e tracciabile da Responsabile di Funzione competente.
3. Le password devono essere modificate al primo accesso, periodicamente ogni tre mesi e in ogni circostanza in cui sussistano dubbi sulla loro riservatezza o compromissione.
4. Le password devono presentare idonei requisiti di complessità:
    a. almeno 9 caratteri
    b. almeno una lettera maiuscola
    c. almeno un carattere speciale
    d. almeno un numero
    e. non devono contenere porzioni della user id o del nome
5. Agli utenti incaricati vengono impartite dal Referente Privacy di Riferimento, istruzioni adeguate affinché adottino le necessarie cautele finalizzate ad assicurare la riservatezza delle proprie password nonché la diligente custodia di eventuali dispositivi (token) di autenticazione.
6. Qualora un utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Referente Privacy e all'Amministratore di Sistema che provvederà alla rigenerazione di una nuova password di primo accesso per l'interessato.
7. Gli account non utilizzati da oltre sei mesi devono essere sospesi ad eccezione di quelli preventivamente autorizzate per mero scopo di gestione tecnica;
8. L'utente è tenuto a garantire la riservatezza delle proprie password custodendole
9. L'utente è responsabile dell'utilizzo delle proprie credenziali così come delle operazioni che, in

10. virtù della autenticazione tramite esse, vengono compiute.

24 Attività di controllo

1. E' fatto salvo il diritto del datore di lavoro di effettuare controlli sull'utilizzo degli strumenti ICT del lavoratore, quando ciò sia dettato da:
    a. esigenze per l'esercizio o la difesa in sede giudiziaria:
    b. riscontri di gravi inadempienze della prestazione lavorativa;
    c. da oggettivi indizi di commissione di illeciti;
    d. esigenze di salvaguardia della vita o della incolumità di terzi;
    e. Norme specifiche di Legge o disposizioni della Autorità Giudiziaria;
    f. da esigenze organizzative, produttive, di sicurezza ed il mancato rispetto del presente regolamento che evidenzino comportamenti anomali (evento dannoso, situazione di pericolo, rischi di responsabilità per la Società).
    g. la verifica sui comportamenti anomali è effettuata con controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa (o ad un determinata area funzionale);
    h. il controllo può concludersi con avviso generalizzato sul rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle disposizioni impartite;
    i. in caso di reiterazione delle anomalie, i controlli potranno assumere carattere mirato
    j. non saranno effettuati controlli prolungati, costanti o indiscriminati.

25 Classificazione dei dati trattati

1. Al fine di conseguire una corretta gestione dei dati viene definita una gerarchia di conoscibilità sia in termini generali che più specificamente in relazione agli obblighi di Legge derivanti dalla tutela dei dati personali. E', quindi, necessario procedere ad una classificazione dei dati anche nell'ottica di dover contemporaneamente definire le politiche di accesso agli stessi. La classificazione dei dati è indispensabile nel momento in cui il trattamento avviene tramite l'uso delle tecnologie dell'informazione.
2. Devono, in ogni caso, essere rispettate le Norme sulla tutela dei dati personali, accesso ai documenti amministrativi, sulla tutela del segreto e divieto di divulgazione.
3. La classificazione, in generale, avviene in base alle esigenze operative, alla normativa vigente e a tutto ciò che fa parte del "modus operandi" aziendale.

4. Parallelamente alla individuazione delle tipologie di dato previste dal Regolamento Europeo UE 2016/679 agli artt.4,9 4 10 (dato personale, dato particolare, dato giudiziario), ai fini della pianificazione della sicurezza delle informazioni aziendali, si adotta il seguente schema di classificazione:
    a. Dato pubblico
    b. Dato tecnico (dati progettuali o operativi)
    c. Dato amministrativo (ordini, fatture, contabilità);
    d. Dati relativi alle risorse umane (contratti, inquadramenti, permessi, orari, etc.)
    e. Dato riservato
    f. Dato strategico
5. Dal punto di vista dei requisiti di riservatezza si adottano misure diverse a seconda del livello di classificazione:
    a. per il dato pubblico si adottano, quantomeno, le misure minime di sicurezza (autenticazione, autorizzazione, antimalware, filtro web e firewall);
    b. per il dato tecnico si adottano misure di riservatezza superiori al livello a) mantenendo l'accesso ai soli soggetti cui compete la visualizzazione e abilitando la modifica ad un numero ristretto di soggetti;
    c. il dato amministrativo viene tutelato con misure più stringenti di quelle previste al livello b), abilitando accesso e modifica esclusivamente alla struttura aziendale competente;
    d. il dato di livello d) viene tutelato come il dato di livello c) con l'aggiunta di ulteriori misure fisiche, tecniche ed informatiche;
    e. il dato di livello e) è riservato ai soli vertici aziendali ed è oggetto di speciali misure finalizzate alla riservatezza (protezione con password, protocolli sicuri, crittografia);
    f. il dato di categoria f) (dato strategico) è riservato ai soli membri del Consiglio di Amministrazione aziendale.

26 Conservazione dei dati

1. In ossequio al principio di finalità i sistemi software devono essere programmati, configurati o utilizzati in modo da cancellare periodicamente ed automaticamente i dati relativi agli accessi ad Internet e al traffico telematico.
2. Eccezionalmente la conservazione può essere protratta, per il tempo indispensabile e per le sole informazioni necessarie, in relazione a:
    - esigenze tecniche o di sicurezza particolari,

- indispensabilità dei dati rispetto all'esercizio o difesa in sede giudiziaria
- obbligo di custodire i dati per una specifica richiesta dell'Autorità Giudiziaria.

3. Negli atti di acquisizione di forniture e servizi relativi ai software applicativi, devono essere previste esplicite clausole relative ai concetti di privacy by design, privacy by default e data retention.

27 Amministratore di Sistema

1. La figura dell'amministratore di sistema è oggetto di uno specifico provvedimento del Garante della Privacy in quanto lo svolgimento delle mansioni di un amministratore di sistema, anche a seguito di una sua formale designazione quale responsabile o incaricato del trattamento, comporta di regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti.
2. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità e, a i sensi dell'art.32 del Regolamento UE 2016/679, sono tenuti ad adottare idonee misure di sicurezza.
3. Ai sensi dell'art. 2- quaterdecies del D.Lgs. 10 Agosto 2018, n. 101, il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
4. l'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti per cui l'attribuzione delle funzioni di amministratore di sistema deve avvenire:
    a. previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
    b. su base individuale e nominativa e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
5. Ai fini del presente regolamento, ed in conformità con il Provvedimento del 27 Novembre 2008 successivamente modificato, con la definizione di "Amministratore di Sistema" si individuano figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue

componenti nonché figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning), le reti locali, gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

6. Gli Amministratori di Sistema, così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.
7. I principali compiti di un Amministratore di Sistema sono i seguenti:
    a. Monitorare l'infrastruttura ICT di competenza per identificare e prevenire potenziali problemi
    b. Introdurre ed integrare nuove tecnologie negli ambienti esistenti;
    c. Installare e configurare nuovo hardware/software sia lato client sia lato server;
    d. Applicare le patch e gli aggiornamenti necessari al software di base ed applicativo, modificare le configurazioni in base alle esigenze aziendali;
    e. Gestire e tenere aggiornati gli account utente ed i relativi profili di autorizzazione;
    f. Pianificare e verificare la corretta esecuzione dei backup e delle repliche;
    g. Documentare le operazioni effettuate, le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni ai problemi;
    h. Ottenere le migliori prestazioni possibili con l'hardware a disposizione;
    i. Operare secondo le prescrizioni di sicurezza e le procedure interne previste.
    j. Rimettere una relazione annuale al Titolare sui principali eventi che hanno caratterizzato l'infrastruttura e su eventuali criticità e violazioni di sicurezza.
8. Il Titolare del trattamento è tenuto a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti.

28 Richieste di assistenza

1. Le richieste di assistenza da parte degli utenti delle Postazioni di Lavoro e dei Servizi Applicativi aziendali devono avere luogo, salvo che il disservizio/malfunzionamento riguardi esclusivamente quest'ultima, attraverso la piattaforma telematica di Help Desk messa a disposizione;
2. Le segnalazioni devono essere, di norma, inoltrate dal Responsabile/referente dell'ufficio interessato e devono essere puntuali e circostanziate.

29 Formazione

1. Sono periodicamente previste specifiche attività di formazione ed aggiornamento sulle procedure aziendali di sicurezza informatica per tutti gli utenti interni e, dove rilevante, per utenti terzi.
2. Sono periodicamente svolti corsi di aggiornamento relativi alle competenze digitali e all'utilizzo degli strumenti informatici per l'attività lavorativa.

30 Cessazione del rapporto di lavoro

1. In caso di cessazione/conclusione del rapporto di lavoro (a qualsiasi titolo) con l'azienda, l'utente ha l'obbligo di:
    a. Restituire i beni mobili e strumentali in dotazione per l'attività lavorativa (notebook, smartphone, pendrive, etc.) già privati di qualsiasi dato o documento personale;
    b. Riconsegnare integri e completi eventuali dati e programmi aziendali utilizzati per la prestazione lavorativa.
    c. Cancellare dalla casella email aziendale qualsiasi contenuto di carattere personale e consegnare le credenziali al Titolare che provvederà, eventualmente tramite l'Amministratore di Sistema, alla archiviazione dei contenuti aziendali e alla disabilitazione della casella stessa al termine di sette giorni solari
2. L'utente viene destituito da tutte le prerogative di accesso ed utilizzo delle risorse ICT aziendali: in tal senso l'Ufficio Risorse Umane è tenuto a dare pronta comunicazione della cessazione del rapporto all'Amministratore di Sistema, ai fini della disabilitazione delle credenziali di accesso.

31 Sanzioni

1. La mancata osservanza delle disposizioni del presente regolamento comporta sanzioni, graduate in base alla gravità della violazione in linea a quanto previsto dal contratto collettivo di lavoro applicato;
2. L'irrogazione delle suddette sanzioni non preclude, né pregiudica l'azione giudiziaria del Titolare di denuncia di atti illeciti di rilevanza penale o di risarcimento civile per danni al patrimonio o all'immagine della Società.

32 ALLEGATI

32.1 Allegato 1 – firma messaggi di posta

--
Ing. Mariano Paolizzi
Ufficio Tecnico - ICT
tel: 0861 43961
fax: 0861 211346
ufficiogestioneambientale@teramoambiente.it
ufficiotecnico@teramoambiente.it
ict@teramoambiente.it

TERAMO AMBIENTE

Via M.Delfico, 73
64100, Teramo (TE)
Telefono: 0861 43961
Fax: 0861 211346

Member of CISQ Federation
RINA
CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001