Rosa dei Venti
A.P.S.P.

REVISIONE DEL DISCIPLINARE AZIENDALE PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI DA PARTE DEI DIPENDENTI E DEI COLLABORATORI

INDICE

PREMESSA

L'Azienda Pubblica di Servizi alla Persona "Rosa dei Venti", di seguito denominata "Titolare del trattamento" o "Amministrazione", nell'espletamento della sua attività opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative

volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

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

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

Le indicazioni contenute nel presente documento tengono altresì conto del principio di responsabilizzazione c.d. "accountability" definito dal Regolamento Ue 16/679.

Il presente disciplinare viene adottato sulla base delle indicazioni contenute nel provvedimento generale del Garante per la protezione dei dati personali di data 1 marzo 2007, n. 13 ("Lavoro: le linee guida del Garante per posta elettronica e internet", G.U. n. 58 del 10 marzo 2007) ed ha per oggetto la definizione dei criteri e delle modalità operative di accesso ed utilizzo degli strumenti informatici, tra cui la rete Internet e il sistema di posta elettronica, da parte dei propri dipendenti e collaboratori.

Il presente documento è stato redatto tenuto conto degli obblighi di "adeguata informazione" prescritti dall'articolo 4, della legge n. 300/1970, come riscritto dall'art. 23 del d.lgs. n. 151/2015 ed entra in vigore nella data della sua sottoscrizione.

Il Titolare del Trattamento ha autorizzato la società Gananet di Ganarini Paolo quale responsabile del trattamento ex art. 28 GDPR, a compiere interventi tecnici e/o manutentori diretti a garantire la sicurezza e la salvaguardia del proprio sistema informatico (manutenzione e implementazione hardware/software e monitoraggio).

Sono inoltre stati individuati gli amministratori di sistema, le cui competenze sono descritte nei documenti di nomina agli atti, accessibili mediante richiesta rivolta agli uffici amministrativi.

1. FINALITÀ E CONTESTO NORMATIVO

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

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

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

- Codice penale, con particolare riferimento ai reati informatici;
- L. 300/1970 (Statuto dei lavoratori) - artt. 4, 7 e 8 come riscritto dall'art. 23 del d.lgs. n. 151/2015 ed entra in vigore nella data della sua sottoscrizione;
- D. Lgs. 196/2003 e s.m. (Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);

- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per posta elettronica e Internet" di cui alla deliberazione 13/2007 ed ha per oggetto la definizione dei criteri e delle modalità operative di accesso ed utilizzo degli strumenti informatici, tra cui la rete Internet e il sistema di posta elettronica, da parte dei propri dipendenti e collaboratori;
- D. Lgs. 81/2008 e s.m.i (Testo Unico sulla sicurezza);
- D.P.R. 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione);
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR).

2. DEFINIZIONI

POSTAZIONE DI LAVORO (CLIENT): personal computer, PC portatile o thin-client collegato alla rete informatica del titolare tramite il quale l'utente accede ai servizi informatici.
UTENTE DI POSTA ELETTRONICA: persona autorizzata ad accedere al servizio di posta elettronica.
LOG: archivio delle attività effettuate in rete dall'utente.
CREDENZIALI DI AUTENTICAZIONE: codice utente e password richiesti dal sistema o dalla postazione di lavoro per verificare se l'utente è autorizzato ad accedere e con quali modalità.
WHITE LIST: elenco di siti che il datore di lavoro ritiene comunemente attinenti all'attività lavorativa svolta.
BLACK LIST: elenco di siti che presentano contenuti non attinenti all'attività lavorativa e, per questa ragione, sottoposti a filtri che si attivano qualora l'utente cerchi di accedervi.
TITOLARE DEL TRATTAMENTO: 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 (art. 4 Reg UE 16/679).
INCARICATO: persona fisica autorizzata dal titolare o dal responsabile a compiere operazioni di trattamento di dati personali.
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 ex art. 28 GDPR.
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 (art. 4 Reg UE 16/679).
AMMINISTRATORI DI SISTEMA: figura professionale finalizzata alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009.
FILE DI LOG: registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato.
STRUMENTI INFORMATICI: personal computer fissi o portatili, stampanti locali o di rete, programmi e prodotti software, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc).

3. PRINCIPI GENERALI

Gli strumenti informatici sono assegnati agli Utenti unicamente per lo svolgimento dell'attività lavorativa e devono essere utilizzati con modalità e mediante comportamenti adeguati ai compiti assegnati e alle responsabilità connesse, nel rispetto del Codice di comportamento dei dipendenti della pubblica amministrazione e delle normative e direttive interne.
È vietato l'utilizzo di ogni strumento aziendale per attività non afferente all'esercizio dei compiti e delle mansioni affidate.
Nell'esecuzione della propria attività lavorativa, gli Utenti sono tenuti ad attenersi alle seguenti istruzioni generali:

a) effettuare la propria attività uniformandosi alle disposizioni della Amministrazione e alle istruzioni ricevute;
b) custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente alla Direzione ogni danneggiamento, smarrimento o furto;
c) mantenere la riservatezza sulle informazioni e sui dati personali di cui siano venuti a conoscenza durante lo svolgimento della propria attività;
d) in caso di cessazione dal servizio o dalla prestazione svolta per la Amministrazione, astenersi dalla comunicazione a terzi e dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività;
e) adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati così come di accesso agli stessi da parte di soggetti non autorizzati.

4. REGOLE PER L'UTILIZZO DEI SISTEMI INFORMATICI

L'accesso alle applicazioni del sistema informativo della Amministrazione deve sempre avvenire attraverso autenticazione mediante credenziali di dominio.
Le credenziali di autenticazione, da gestire nel rispetto delle regole stabilite, sono strettamente personali e non devono essere comunicate né rese disponibili ad altri soggetti. In caso di diffusione accidentale, anche solo presunta, le password devono essere immediatamente modificate e l'incidente va immediatamente segnalato alla Direzione.

5. UTILIZZO DELLA RETE E DEL PERSONAL COMPUTER

L'utilizzo di tutti gli strumenti informatici di proprietà del Titolare deve avvenire osservando regole di buona diligenza e prudenza, con senso di responsabilità e seguendo le istruzioni impartite dal Titolare e dalle persone delegate.
L'uso degli strumenti informatici aziendali (PC, attrezzatura informatica, notebook, accesso alla rete internet, telefoni mobili, ecc.) è consentito unicamente agli utenti autorizzati mediante attribuzione di apposito incarico al trattamento. Ogni utilizzo dei predetti beni non inerente all'attività lavorativa è tassativamente vietato.
Le unità di rete sono aree di condivisione di dati ed informazioni strettamente legati all'attività lavorativa. I file ivi dislocati devono avere attinenza con le attività svolte da ciascun incaricato e qualunque file che non sia legato all'attività lavorativa non può essere ivi dislocato, nemmeno per brevi periodi. Le cartelle utenti presenti nei server sono aree di condivisione di informazioni strettamente lavorative e non possono in alcun modo essere utilizzate per scopi diversi.
Ogni utente è responsabile per l'uso riferito al proprio account ed è personalmente tenuto a conformarsi a modalità di utilizzo atte ad impedire accessi da parte di terzi non autorizzati. Non è ammessa la comunicazione della propria credenziale d'accesso a terzi.
Le disposizioni di seguito riportate, relative alle credenziali di autenticazione, sono finalizzate a garantire la sicurezza nell'accesso:

a) le credenziali degli utenti permettono l'accesso alle postazioni client assegnate, devono essere composte da almeno 8 caratteri alfanumerici con lettere maiuscole e minuscole e almeno un carattere speciale. Non devono contenere riferimenti che riconducano agevolmente agli incaricati;
b) la password è personale, riservata e non può essere ceduta o comunicata ad alcuno. È pertanto vietato l'uso della password di altri utenti;
c) è obbligatorio modificare la password ogni volta che il sistema ne faccia richiesta o almeno ogni tre mesi;
d) per esigenze operative a carattere d'urgenza o di sicurezza il Titolare, tramite l'Amministratore di Sistema ha facoltà di modificare la password degli utenti;
e) qualsiasi attività svolta utilizzando nome utente e password sarà ricondotta nella sfera di responsabilità dell'utente assegnatario delle credenziali. L'incaricato è civilmente responsabile di ogni danno cagionato al Titolare e/o a terzi, non solo in relazione ai propri fatti illeciti ma anche per quelli commessi da chiunque utilizzi le sue credenziali d'accesso;

Per evitare il pericolo di introdurre virus informatici o di alterare la stabilità delle applicazioni è vietato scaricare ed installare programmi, salva espressa autorizzazione rilasciata da parte del Titolare o dall'Amministratore di Sistema.
Non è consentito modificare le configurazioni del proprio client. Il client deve essere spento al termine dell'attività lavorativa e bloccato con la richiesta di utente/password in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso.
Non è consentito scaricare file contenuti in supporti esterni non aventi alcuna attinenza con la propria prestazione lavorativa.
Qualora un utente dovesse riscontrare malfunzionamenti, guasti o situazioni di rischio per la sicurezza o l'integrità del sistema deve darne immediata comunicazione al Titolare o all'Amministratore di Sistema. Salvo preventiva espressa autorizzazione non è consentito eseguire operazioni di manutenzione ordinaria o straordinaria autonomamente.
Non è consentito archiviare sul proprio client, sul server o su qualunque altra area condivisa, file e dati non inerenti all'attività lavorativa.
È vietato l'uso di supporti di memorizzazione dati esterni (ad es. dischi fissi esterni, chiavette USB, ecc.) per trattare dati e informazioni afferenti l'attività lavorativa.
Il Titolare del trattamento si riserva la facoltà di procedere alla rimozione di ogni applicazione o file ritenuti pericolosi per la sicurezza del sistema, non attinenti all'attività lavorativa o acquisiti ed installati in violazione del presente disciplinare, sia sui clienti degli incaricati sia sulle unità di rete.
L'utente deve limitare le stampe ai dati strettamente necessari, ritirandole prontamente dai vassoi delle stampanti condivise.
In caso di inutilizzo prolungato del client, all'accensione attendere il completamento dell'aggiornamento del sistema di protezione antivirus e procedere ad installare eventuali aggiornamenti proposti.
Agli utenti è fatto espresso divieto di utilizzare qualunque tipo di sistema informatico o elettronico per:

- controllare le attività di altri utenti
- leggere, copiare o cancellare files e software di altri utenti
- utilizzare software rivolti alla violazione della sicurezza del sistema e della privacy
- sostituirsi a terzi nell'uso dei sistemi
- cercare di catturare password altrui o forzare password o comunicazioni criptate
- modificare le configurazioni impostate dall'Amministratore di Sistema
- limitare o negare l'accesso al sistema a utenti legittimi
- effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc.)
- distruggere o alterare dati altrui
- collegare in rete personal computer non di proprietà del titolare
- influenzare negativamente la regolare operatività della rete o interferire con la connettività altrui o con il funzionamento del sistema.

6. UTILIZZO DI DISPOSITIVI MOBILI (NOTEBOOK, TABLET, SMARTPHONE)

L'utente al quale venga assegnato un dispositivo mobile ne è responsabile e dovrà custodirlo con la dovuta diligenza.
In caso di utilizzo all'esterno del luogo di lavoro, il dispositivo dovrà essere custodito con attenzione e conservato in luogo sicuro. La geolocalizzazione su tali dispositivi è disattiva nella modalità predefinita. Qualora l'utente evidenzi che tale modalità è attiva deve segnalare al Responsabile/Titolare del Trattamento o all'Amministratore di sistema che procederà all'immediata disattivazione.
Ai dispositivi mobili si applicano le regole sopra indicate per i PC connessi in rete.
Nella memoria locale dei dispositivi di norma non vanno conservati e archiviati file o cartelle necessari all'attività lavorativa.
All'accensione del dispositivo attendere il completamento di eventuali aggiornamenti del sistema, della protezione antivirus e procedere ad installare gli aggiornamenti proposti. In caso di anomalie segnalare l'accaduto al Responsabile/Titolare del Trattamento o all'Amministratore di sistema.

7. UTILIZZO DELLA RETE INTERNET

L'accesso alla rete Internet può essere effettuato da qualsiasi utente che sia autenticato (credenziali di accesso) su una qualsiasi postazione di lavoro connessa. Il client assegnato al singolo utente ed abilitato alla navigazione Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
Internet è uno strumento di lavoro e quindi è possibile, che il Titolare del Trattamento adotti le seguenti misure in conformità con le previsioni di cui all'art. 32 del GDPR volte a garantire la sicurezza delle informazioni e dei dati personali oggetto di trattamento da parte della Amministrazione:

- individuazione di white list (composte da soli siti istituzionali, rispetto ai quali la navigazione è correlata e funzionale allo svolgimento della prestazione lavorativa)
- individuazione di black list (composte da tutti quei siti che, oltre a non avere attinenza con il lavoro, presentano contenuti non in linea con le politiche di gestione adottate dal titolare)
- impostazione di filtri sul firewall.

È vietato il download di software gratuiti (freeware) e shareware nonché di file video o musicali prelevati da siti Internet, salvi i casi direttamente autorizzati dal titolare.
È vietata ogni forma di registrazione a siti, social, newsletter, blog e quant'altro assimilabile, salvi i casi direttamente autorizzati. È vietata la partecipazione a forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) salvi i casi direttamente autorizzati.
È vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvi i casi direttamente autorizzati.
Non è consentito accedere ed utilizzare la rete internet in modo difforme da quanto previsto dal presente disciplinare e dalle leggi penali, civili ed amministrative in materia. In ogni caso, ogni utente è direttamente responsabile dell'uso del servizio di accesso ad Internet, dei siti ai quali accede, delle informazioni che immette e riceve.
Qualora un utente dovesse riscontrare malfunzionamenti, guasti o situazioni di rischio per la sicurezza o l'integrità del sistema è tenuto a darne immediata comunicazione al Titolare/Responsabile del Trattamento o all'Amministratore di Sistema.

Gli eventuali controlli, compiuti dal Titolare per il tramite dell'Amministratore di sistema, potranno avvenire mediante un sistema di analisi dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.

I dati contenuti nei file di log, relativi agli accessi ad Internet e al traffico telematico, saranno conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza. I file di log potranno essere utilizzati per:
a) la produzione di report statistici che presentino i dati relativi alla navigazione in forma aggregata e anonima;
b) per l'analisi dei problemi riscontrati nel sistema e soluzione dei medesimi, estraendo i dati in modo aggregato e in forma anonima.

Il trattamento dei file di log non sarà mai preordinato all'esercizio di un controllo a distanza sull'attività lavorativa ma, la finalità del trattamento in questione, è volta a garantire la sicurezza informatica della Amministrazione (ad es. rilevare vulnerabilità e/o esigenze di manutenzione) e avrà luogo solo in presenza di anomalie - c.d. "controllo preterintenzionale" o, laddove ve ne sia il presupposto di necessità, per consentire l'accertamento ex post di una presunta condotta illecita. I file stessi, salvo diverse esigenze di tutela o richieste delle autorità di pubblica sicurezza, vengono conservati non oltre un mese, ossia limitatamente al tempo indispensabile per il perseguimento delle finalità sopra richiamate.

Il sistema di posta elettronica è da intendersi quale strumento di lavoro e come tale deve essere utilizzato.
Può essere assegnato un account di posta elettronica ad ogni utente della rete informatica o indirizzi condivisi tra più utenti.
L'accesso al sistema di posta elettronica è protetto dalla richiesta di autenticazione.
Le disposizioni di seguito riportate sono enucleate al fine di garantire un corretto utilizzo dello strumento di posta elettronica:
a) all'utente non è consentito servirsi dell'account fornito dal titolare per l'invio di mail non connesse con l'attività e la mansione svolta (es: mail a contenuto privato, giochi, appelli, petizioni, catene di S. Antonio, ecc.);
b) si deve evitare di allegare materiale potenzialmente insicuro o file di dimensioni eccessive. In quest'ultimo caso si dovranno utilizzare formati compressi (zip, rar, ecc.);
c) nel caso di messaggi dal mittente o dall'oggetto insolito, va fatta la segnalazione all'Amministratore di Sistema ed è vietata l'apertura degli stessi. Lo stesso vale nel caso di messaggi provenienti da mittenti conosciuti che tuttavia presentano allegati con particolari estensioni (es: .exe, .scr, .pif., .bat..);
e) si deve evitare l'invio di mail contenenti allegati con dati "sensibili"; qualora ciò sia necessario per determinate esigenze, gli allegati devono essere criptati e protetti da password di apertura. La password dovrà essere inviata al destinatario per altro mezzo;
f) qualora il messaggio debba essere inviato a più soggetti, i loro indirizzi non vanno condivisi (ed es. mediante inserimento nel campo "CCn");
g) prevedere, in caso di assenza prolungata del lavoratore (es: ferie), l'invio di messaggi di risposta automatica che indichino la durata dell'assenza ed il nominativo del soggetto al quale è possibile rivolgersi;
h) l'iscrizione a mailing list o newsletter è concessa solo per motivi strettamente professionali: prima di iscriversi è necessario l'autorizzazione del titolare;
i) l'intestatario dell'account ha facoltà di delegare ad altri il diritto d'accesso allo strumento in caso di assenza prolungata ai fini di garantire la continuità nell'attività lavorativa anche tramite la procedura aziendale di nomina del fiduciario. Il fiduciario dovrà essere scelto e nominato fra i colleghi e, qualora dovesse accedere alla casella di posta della persona assente, non potrà comunque considerare i messaggi che presentino contenuto non attinente alle motivazioni per cui si effettua l'accesso;
l) l'Amministratore di Sistema può avere accesso all'account a seguito di situazioni che abbiano pregiudicato il funzionamento del sistema.

I documenti inerenti il know how aziendale tecnico o commerciale protetto non possono essere comunicati all'esterno senza la preventiva autorizzazione della Direzione.
L'utente ha l'obbligo di:

- inserire la propria firma per l'invio di messaggi verso l'esterno, uniformando il carattere del corpo del testo e la firma automatica in calce all'email secondo lo stile definito dalla Amministrazione;
- proteggere la privacy dell'interlocutore evitando di inoltrare messaggi altrui in assenza di una adeguata base giuridica;
- evitare di diffondere, all'esterno della Amministrazione, indirizzi di posta elettronica di terzi.

Il contenuto presente nella casella di posta elettronica assegnata al collaboratore sarà conservato dal titolare in costanza del rapporto di lavoro e, successivamente, per il termine di due anni.
Con la cessazione del rapporto di lavoro il datore di lavoro provvederà alla rimozione previa disattivazione della casella di posta assegnata e alla eventuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi; inoltre, la disattivazione sarà eseguita in modo tale da inibire la ricezione di messaggi in entrata e la conservazione degli stessi nei server aziendali.

9. PROTEZIONE ANTIVIRUS

L'utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico del titolare mediante virus o mediante ogni altro software aggressivo.
Qualora il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, spegnere il computer e segnalare l'accaduto all'Amministratore di Sistema.
Non è consentito l'utilizzo di supporti di memorizzazione esterni di provenienza ignota.
In caso di utilizzo autorizzato dei suddetti dispositivi, si dovrà procedere alla verifica degli stessi e nel caso in cui vengano rilevate anomalie alla loro consegna all'Amministratore di Sistema.

10. INTERRUZIONE D'UFFICIO DEL SERVIZIO

Il titolare si riserva di sospendere all'incaricato il servizio di accesso ad Internet e alla posta elettronica nei seguenti casi:

a) qualora venga meno la condizione di dipendente o collaboratore;
b) qualora si accerti un uso non corretto del servizio e degli strumenti informatici messi a disposizione;
c) in caso di manomissioni e/o interventi impropri su hardware/software;
d) in caso di diffusione o di comunicazione imputabile direttamente o indirettamente all'utente relativamente a dati personali o altre informazioni riservate;
e) accesso a directory/file/siti non rientranti fra quelli per cui l'utente abbia autorizzazione.

11. UTILIZZO DEL TELEFONO

Il telefono è uno strumento di lavoro e come tale deve esser utilizzato. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa. Eventuali telefonate a carattere privato potranno essere effettuate con moderazione.
Gli smartphone affidati agli utenti sono strumenti di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa. Gli utenti cui è assegnato uno smartphone aziendale sono responsabili del suo utilizzo e della sua custodia. Allo smartphone aziendale si applicano le medesime regole sopra previste: in particolare è vietato l'utilizzo dello smartphone messo a disposizione per

l'invio o la ricezione di messaggistica di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.
Gli smartphone potrebbero essere dotati della funzionalità di localizzazione geografica. Tale funzione deve essere disattivata dall'utente. È vietato effettuare il Jailbreak del dispositivo e più in generale è vietata qualsiasi procedura di sblocco del device aziendale assegnato, ad esempio, per installare/utilizzare applicazioni non autorizzate.
Se non espressamente autorizzato è vietato l'uso per finalità lavorative e nell'adempimento dei compiti lavorativi di cellulari o tablet diversi da quelli aziendali.

12. SPAZI DI CONDIVISIONE SULLA RETE AZIENDALE

Gli spazi di condivisione devono essere utilizzati per la memorizzazione di file ad uso strettamente lavorativo. I file e i documenti di lavoro devono essere obbligatoriamente memorizzati e conservati nell'osservanza dei criteri di legge ai quali l'Amministrazione deve sottostare nello spazio di condivisione apposito al fine di impedire la perdita di dati aziendali.
In caso di comprovato pericolo per la sicurezza dei sistemi, l'Amministrazione potrà procedere anche senza preavviso alla rimozione di file e/o applicazioni presenti negli spazi di condivisione degli Utenti, dandone successiva e tempestiva comunicazione agli interessati.

13. PROTEZIONE CONTRO FURTI E DANNEGGIAMENTI

Tutti gli strumenti informatici devono essere custoditi in luogo sicuro, adottando le opportune precauzioni contro il furto degli stessi e/o dei dati in essi contenuti. L'Utente è tenuto a informare immediatamente il Direttore qualora vi sia la possibilità di una violazione di dati personali o di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso.

14. SISTEMA DI MONITORAGGIO DI SICUREZZA IT CLOUD

Si forniscono le seguenti informazioni relativamente all'attività conseguente all'installazione, da parte dell'Amministrazione, di un sistema di monitoraggio di sicurezza IT Cloud ad implementazione delle misure di protezione dell'infrastruttura informatica aziendale.
Il servizio sopra richiamato ha come finalità esclusiva quella di favorire la rilevazione in tempo reale di anomalie di sistema al fine di supportare l'Amministrazione e l'Amministratore di Sistema nella riduzione di possibili elementi di rischio insiti nell'utilizzo dei sistemi informatici aziendali, escludendo nel contempo che da ciò possa derivare la possibilità di un illecito controllo a distanza dell'attività dei lavoratori.
La misura di precauzione rappresentata dal sistema di monitoraggio IT tiene conto della natura dell'Amministrazione, della qualità dei dati personali oggetto di trattamento e dei derivanti rischi sui soggetti interessati e l'attività di presidio, per come strutturata, integra una misura di protezione e precauzione a fronte dell'evoluzione della minaccia cibernetica, in particolare incombente sulla pubblica amministrazione.
Il presupposto di liceità del servizio di monitoraggio IT e dei relativi trattamenti è riconducibile sia alle disposizioni del GDPR, che stabilisce per il titolare del trattamento l'obbligo di mettere in atto "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio", (artt. 24 e 32) che alle "Misure minime di sicurezza ICT per le pubbliche amministrazioni" definite da AGID.
Nello specifico il predetto servizio prevede l'inventario dei client aziendali e l'installazione su ciascuno di essi di un sistema di monitoraggio riguardante la configurazione del sistema operativo e dei software presenti (attività che non rientrano tra quelle di competenza del personale autorizzato all'uso dei client). Il monitoraggio IT ha luogo mediante l'attivazione di software di ricognizione (agent) sui

singoli client che trasmettono automaticamente (due/tre volte al giorno) le predette informazioni ad una "consolle" presidiata da parte di tecnici preposti alla loro analisi e l'individuazione di possibili vulnerabilità su cui si potrà intervenire a mitigazione dei rischi che ne possano derivare.
Le informazioni alle quali l'agent attinge riguardano:
a) il registro di sistema di Windows (l'elenco dei software installati con relativa versione, per individuare le possibili vulnerabilità); le policy di gruppo (impostazioni del sistema operativo);
b) l'output di alcuni comandi di sistema (per esempio per verificare se l'account "Guest" è attivo o no).
Le eventuali criticità oggetto di rilevazione sono le seguenti:
a) le vulnerabilità dei software in base alla versione specifica di tutti i programmi installati e alle "porte aperte" della macchina in uso; le configurazioni e le versioni del sistema operativo utilizzato nonché le applicazioni istallate ed il relativo livello di patch;
b) gli eventi di sistema potenzialmente legati ad azioni maligne (ad es. aggiunta di utenti amministratori o modifica di parametri di sicurezza o installazione/disinstallazione di software).
Tali informazioni saranno processate in tempo reale e le vulnerabilità che dovessero emergere saranno segnalate mediante report dedicati rivolti all'Amministratore di sistema per favorire gli interventi di mitigazione.
Per quanto riguarda i tempi di elaborazione delle informazioni raccolte, il monitoraggio IT non prevede la conservazione dei dati acquisiti e la rappresentazione di ciascun dispositivo viene sempre aggiornata per effetto dell'ultima rilevazione.
La raccolta di queste informazioni potrebbe prevedere l'identificazione dei soggetti assegnatari del client aziendale laddove vi sia una correlazione tra la catalogazione del dispositivo (client) con il dato identificativo dell'utilizzatore. Al ricorrere di tale circostanza, il monitoraggio IT potrebbe consentire una correlazione tra le operazioni eseguite dall'utilizzatore sul dispositivo di cui affidatario limitatamente alle informazioni alle quali l'agent attinge e, di conseguenza, rappresentare un'ipotesi di controllo sull'utilizzo che i collaboratori fanno degli strumenti informatici aziendali limitatamente a tali ipotesi.
Le informazioni raccolte nel contesto del monitoraggio di sicurezza IT non saranno mai utilizzate per trattamenti ulteriori e/o per finalità diverse da quelle sopra richiamate.

15. STRUMENTI ASSEGNATI AI DIPENDENTI PER RENDERE LA PRESTAZIONE LAVORATIVA

Ai dipendenti vengono messi a disposizione i seguenti strumenti:

- PC
- Note book
- Tablet – in uso al solo servizio animazione
- Smartphone – in uso al centro diurno

L'utilizzo di PC e dispositivi mobili assegnati dall'Amministrazione ai Collaboratori è generalmente normato dai punti 5 e 6 del presente documento.
Il salvataggio di informazioni personali dei Collaboratori non inerenti l'attività lavorativa sui dispositivi assegnati è vietato, salvo autorizzazione specifica da parte dell'Amministrazione. Al cessare dell'attività lavorativa o in seguito alla sostituzione della postazione o del dispositivo assegnato, tutti i file utente vengono rimossi dal dispositivo prima della riassegnazione.
Lo smaltimento dei dispositivi che raggiungono il termine della loro vita utile viene gestito come da best practice del settore, tramite sovrascrittura e/o distruzione fisica dei supporti di archiviazione.
Smartphone e tablet possono essere gestiti centralmente tramite una piattaforma Cloud di amministrazione del parco mobile aziendale, nel pieno rispetto della normativa vigente in materia di privacy.

16. CONTROLLI E SANZIONI DISCIPLINARI

Sono interdetti al datore di lavoro controlli del personale dipendente effettuati in maniera diretta, prolungata, costante o indiscriminata (art. 4, Statuto dei lavoratori, l. 300/1970).
Ciò premesso, per motivi di sicurezza del sistema informatico o per indifferibili esigenze tecniche e/o di manutenzione (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, adozione di misure di sicurezza sugli apparati, etc.), comunque estranei a qualsiasi finalità di controllo diretto dell'attività lavorativa, è facoltà del titolare tramite l'Amministratore di sistema, accedere, nel rispetto della normativa vigente, agli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.
L'accesso, laddove vi sia il presupposto della necessità, potrà altresì aver luogo nell'esercizio dei "controlli difensivi" che competono al datore di lavoro per consentire l'accertamento ex post di una presunta condotta illecita dei propri collaboratori. In particolare, gli eventuali controlli si svolgeranno in modo lecito, corretto e trasparente e saranno posti in essere unicamente per il perseguimento delle predette finalità.
Tali controlli saranno effettuati qualora le misure minime preventivamente esposte non siano state sufficienti, adottando soluzioni tecnologiche idonee a garantire i profili di sicurezza dei sistemi informativi e dei dati personali trattati con il bilanciamento dei diritti dei lavoratori coinvolti.
I controlli saranno svolti con gradualità, secondo i principi di pertinenza e non eccedenza. In seguito si espongono le modalità di esercizio di tali controlli: in prima battuta si effettuerà un controllo preliminare su dati anonimi ed aggregati; si procederà pertanto con verifiche di ufficio o gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole prestabilite.
Il controllo anonimo può dare atto ad un avviso di rilevazione di un utilizzo inadeguato degli strumenti aziendali; contestualmente si diramerà una nota di richiamo invitando tutti i dipendenti e collaboratori ad attenersi ai compiti e alle mansioni impartite tenuto conto del dovere di conformarsi alle presenti regole. Se si dovesse ripetere l'anomalia sarà facoltà dell'Amministrazione procedere con controlli mirati, anche su base individuale, e successivamente, in caso di infrazioni, adottare sanzioni disciplinari.
L'Amministratore di Sistema, nel caso in cui rilevi anomalie o configurazioni non corrette, può provvedere a isolare immediatamente l'origine dell'anomalia o del malfunzionamento anche senza preavvisare l'Utente, per salvaguardare la sicurezza e l'integrità dei sistemi informativi dell'Amministrazione.
L'adozione delle sanzioni disciplinari avverrà a norma dell'art. 2106 c.c. del codice civile, dell'art. 7 dello statuto dei lavoratori (legge 300/1970), del contratto di riferimento e del relativo codice disciplinare vigente.

17. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

Oltre al rispetto del presente disciplinare è fatto obbligo di attenersi scrupolosamente alle disposizioni in materia di trattamento dati personali e alle relative misure di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento e nel materiale formativo messo a disposizione di ciascun collaboratore e dipendente osservando con attenzione le prescrizioni del Reg. UE 16/679.
Ciascun incaricato assume la piena responsabilità nel merito dell'osservanza del modello organizzativo, delle misure di sicurezza, delle indicazioni fornite dall'Amministrazione, dall'Amministratore di Sistema e dal DPO.
Ciascun incaricato è tenuto a mantenere un costante flusso informativo con l'Amministratore di Sistema e con il DPO segnalando ogni eventuale criticità o violazione sul sistema di sicurezza adottato.

18. AGGIORNAMENTO E REVISIONE DEL DISCIPLINARE INTERNO

Il presente Disciplinare è soggetto a verifica con eventuali revisioni ed aggiornamenti in caso di modifiche e/o integrazioni della normativa di legge.
Il presente disciplinare viene consegnato al personale dipendente dell'Amministrazione ai sensi e per gli effetti dell'art. 7 legge 10 maggio 1970 n. 300 in relazione al codice di comportamento di dipendenti del quale costituisce parte integrante.

Borgo Chiese, lì 27 ottobre 2025

Il Presidente
dott. Christian Sartori