REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI E PER LA TUTELA DELLE INFORMAZIONI

INFORMAZIONI SUL DOCUMENTO	
Ente	Azienda Servizi alla Persona Opus Civium, di seguito anche ASP
Revisione	Rev. 0
Data	25/03/2026
Commenti:	Revisione n.0 – Prima pubblicazione
Stato:	◉ Valido ◎ Ritirato
Lingua:	Italiano
Redatto da:	Galli Gregorio (Galli Data Service – Società Esterna)
Revisionato da:	Piazza Barbara (ASP-OC, Direttore Generale) Caiazzo Gaetana (ASP-OC, Istruttore Ufficio Acquisti)
Approvato da:	Consiglio di Amministrazione
Possibile conservazione, validazione e diffusione in formato digitale	

INDICE

INTRODUZIONE

A) Premesse e scopo del regolamento La progressiva diffusione delle tecnologie informatiche espone ormai i sistemi informativi di qualsiasi organizzazione a rischi di carattere legale, sia penale che civile, creando altresì diversi problemi di sicurezza e di immagine. Il patrimonio informativo è un bene "critico" per l'Ente, che deve essere correttamente gestito e protetto, adottando le misure di sicurezza più adeguate e controllandone costantemente l'efficacia. Ciò non solo per operare in conformità alle leggi vigenti (sempre più stringenti in materia di crimini informatici, protezione dei dati personali e diritto d'autore), ma altresì al fine di perseguire un efficace sistema di gestione per la sicurezza delle informazioni. Il presente documento (di seguito: "Regolamento") soddisfa quindi la necessità di disciplinare le condizioni per il corretto utilizzo del sistema informativo e contiene informazioni indispensabili per comprendere le azioni che possono essere intraprese per contribuire a garantire l'efficace perseguimento degli obiettivi dell'Ente ed a tutela della sicurezza delle informazioni trattate. Questo regolamento viene introdotto nell'intento di perseguire i seguenti scopi:

- garantire la massima sicurezza nell'accesso e nell'utilizzo dei sistemi informatici, nonché la tutela delle informazioni e dei dati elettronici;
- garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche per l'elaborazione dei dati personali e sensibili (principalmente Regolamento UE 2016/679 "General Data Protection Regulation" di seguito GDPR);
- informare con chiarezza i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli;
- garantire la massima efficienza delle risorse del Sistema Informativo e la massima disponibilità di servizio nell'interesse della produttività dell'Ente.

B) Normative di riferimento Il presente regolamento è redatto in conformità al GDPR, considerato quale modello internazionale di riferimento per l'adozione di adeguate misure a tutela della protezione e riservatezza dei dati. Si ritiene inoltre redatto in conformità e valido a recepire i requisiti delle seguenti normative:

- D.Lgs. n. 196/2003 (Codice Privacy) come modificato ed integrato da D.Lgs.101/2018;
- Linee guida per posta elettronica e internet (Garante Privacy marzo 2007);
- Legge n. 300/1970 (Statuto dei Lavoratori) come modificato da D.Lgs.151/2015 (Jobs Act);
- Legge n. 633/1941 (Diritto d'autore) e successive modifiche;
- D.Lgs. n. 231/2001 (Responsabilità amministrativa degli enti).
- Codice Penale Art. 594 (Ingiuria), 595 (Diffamazione), 615 ter (Accesso abusivo ad un sistema informatico o telematico), 615 quater (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici), 615 quinques (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico), 616 (Violazione, sottrazione e soppressione di corrispondenza), 640 ter (Frode informatica);
- Codice Civile Art. 2105 e 2106 del e Codice della Proprietà Industriale Art. 98 e 99 (norme relative alle informazioni coperte da segreto).

Il rispetto delle indicazioni del presente Regolamento consente agli utenti di prevenire il rischio di commettere illeciti riferiti alle suddette normative, che potrebbero comportare gravi responsabilità personali, quali:

- violazioni privacy e trattamento illecito di dati;
- reati informatici (quali accesso abusivo ad un sistema informatico, detenzione e diffusione abusiva di codici di accesso, diffusione di programmi atti a danneggiare o interrompere un sistema informatico, frode informatica, …);
- altri reati quali ingiuria, diffamazione, violazione corrispondenza, detenzione o diffusione di materiale pedopornografico;
- violazione del diritto d'autore e della proprietà intellettuale.

A completamento delle istruzioni si fornisce, in appendice:

- indicazioni di sintesi per la prevenzione di reati informatici (Appendice1);
- indicazioni di sintesi per la prevenzione di violazioni del diritto d'autore (Appendice2);
- copia della nuova formulazione dell'Art.4 dello Statuto dei lavoratori (Appendice3);
- informativa sul trattamento dei dati stoccati nelle infrastrutture IT (Appendice4).

C) Ambito di applicazione Il presente Regolamento è adottato dall' "Azienda Pubblica di Servizi alla Persona Opus Civium" (di seguito anche ASP). Il presente Regolamento si applica presso tutte le strutture/servizi che fanno capo ad ASP. E' tenuto al rispetto del presente regolamento, qualsiasi UTENTE che utilizzi STRUMENTI INFORMATICI, come in seguito definiti.

Per UTENTE si intendono sia i dipendenti a tempo determinato e indeterminato, i lavoratori somministrati, nonché eventuali tirocinanti, stagisti, collaboratori e professionisti che collaborano con l'Azienda:

- che utilizzano uno STRUMENTO INFORMATICO (hardware/software) di proprietà dell'Ente;
- dotati di indirizzo di posta elettronica dell'Ente;
- abilitati all'accesso ad internet tramite connessione dell'Ente;

- abilitati all'accesso alla rete dell'Ente (anche da remoto)

Restano esclusi dal presente regolamento:
- utilizzatori occasionali delle reti wifi, per la quali vige un'apposita regolamentazione;
- società di supporto sistemistico e/o applicativo IT, per la quali vigono apposite garanzie contrattuali.

Per STRUMENTI INFORMATICI si intende:
- la rete informatica LAN;
- lo strumento della posta elettronica con domini di gruppo (es: dominio ASP, messaggistica portale Advenia, ulteriori domini email autorizzati, ecc.);
- l'accesso alla rete internet;
- il personal computer (fisso o portatile) ed i server;
- il software operativo (programmi e/o applicazioni);
- le eventuali periferiche (stampanti, multifunzione, fax, ecc) o altri dispositivi elettronici;
- gli apparati di comunicazione fissi (centralino, telefoni, ecc.) e wi-fi;
- i mobile device quali smartphone, tablet e palmari.

Al fine di presidiare la tutela dell'intero patrimonio informativo dell'Ente si ritiene di inserire nel presente Regolamento un apposito paragrafo contenente le regole di utilizzo della **documentazione cartacea** (da intendersi pertanto inclusa anche nelle prescrizioni generali relative agli strumenti elettronici).

D) Pertinenza delle regole All'interno del quadro generale delineato dal Regolamento, gli utenti sono tenuti a rispettare le prescrizioni aventi pertinenza con il proprio ambito lavorativo (presente o futuro) e con le funzionalità messe a disposizione dall'Ente.

E) Entrata in vigore, divulgazione e responsabilità Il presente Regolamento entra in vigore al momento della sua divulgazione agli utenti, sostituendo qualsiasi indicazione precedente sull'utilizzo degli strumenti elettronici.

Il regolamento, implementato per il perseguimento di obiettivi di efficienza dell'Ente, è redatto in conformità ed in applicazione delle normative di cui al precedente par.B, pertanto non è oggetto di approvazione da parte dell'utente come identificato al punto C), ma di semplice presa visione. Si sottolinea che l'utente è direttamente responsabile di qualsiasi conseguenza derivante da comportamenti difformi dalle indicazioni impartite.

ART.1: Uso responsabile degli strumenti

1.1 Finalità d'utilizzo Gli strumenti elettronici affidati agli utenti sono **strumenti di lavoro**. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

1.2 Buon uso Si richiede l'utilizzo degli strumenti elettronici assegnati assicurandone l'integrità, la conservazione e la sicurezza, evitando comportamenti che possano compromettere la funzionalità, le impostazioni e la sicurezza delle macchine. Si richiede la segnalazione puntuale di eventuali malfunzionamenti o anomalie degli strumenti elettronici in uso. Si richiede lo spegnimento del computer (desktop e notebook) al termine della giornata lavorativa o in caso di prolungata assenza dalla postazione.

1.3 Impostazioni predefinite **Si richiede di NON effettuare sostanziali modifiche del proprio ambiente informatico, con particolare riferimento all'installazione/disinstallazione di applicativi e configurazioni di sistema, se non preventivamente autorizzati. Si richiede inoltre di non** utilizzare gli STRUMENTI INFORMATICI in modo difforme da quanto previsto dal presente regolamento, né per scopi incompatibili con le mansioni lavorative assegnate.

ART.2: Soggetti deputati all'accesso/gestione del sistema informatico

2.1 Soggetti preposti ASP si riserva la possibilità di designare soggetti preposti alla gestione dei sistemi informativi, anche dotati di privilegi di administrator su macchine e sistemi (di seguito definiti anche AdS). Tali soggetti (che possono essere dipendenti interni o società/consulenti esterni) sono deputati alla manutenzione/sviluppo dell'infrastruttura informatica, nonché al supporto agli utenti, attività che potranno comportare l'accesso ai dati memorizzati negli STRUMENTI INFORMATICI.

2.2 Affidabilità dei soggetti Per effettuare tali attività i soggetti preposti sono appositamente nominati, autorizzati ed istruiti dalla Direzione, nonché opportunamente monitorati. Gli utenti possono richiedere in qualunque momento, senza formalità, gli estremi identificativi di tali soggetti.

2.3 Attività consentite L'accesso ai desktop degli utenti da parte degli AdS (o da consulenti esterni preposti all'assistenza su applicativi) può avvenire, per fini di sicurezza, supporto e sviluppo, previa abilitazione da parte dell'utente, anche da remoto attraverso apposite applicazioni (Es: desktop remoto, team-viewer) che mostrano chiaramente all'utente l'accesso in corso. Al fine di garantire la sicurezza dell'infrastruttura l'AdS può effettuare interventi mirati a:

- impostare permessi di accesso (anche differenziati) alla rete ed alla navigazione;
- bloccare l'installazione di applicativi non verificati ed autorizzati;
- bloccare l'accesso a funzionalità di sistema dei computer;
- rimuovere qualsiasi contenuto che venga ritenuto pericoloso e gestire modifiche sulle directory;
- spostare file che possano compromettere il buon funzionamento della rete.

ART.3: Protezione dei database e proprietà dei contenuti

Ogni materiale informatico (documenti, comunicazioni, elenchi, files, directory, database, ecc.) prodotto o acquisito dagli utenti nel corso dell'attività lavorativa tramite apparecchiature fornite da ASP è da intendersi di **proprietà di ASP stessa**, che potrà utilizzarli a sua discrezione (in conformità delle vigenti normative). **In generale è fatto divieto a qualunque soggetto di distruggere, sottrarre, manipolare, divulgare il contenuto delle banche dati se non espressamente autorizzato dalla Direzione.**

In particolare, in merito ai dati personali (informazioni riconducibili a persona fisica, quale collega, cliente, fornitore, referente, collaboratore, visitatore, ecc.), gli utenti sono tenuti a rispettare le indicazioni di riservatezza contenute nella lettera di autorizzazione privacy, accedendo solo ai dati necessari alle mansioni lavorative, garantendo un adeguato livello di protezione e riservatezza.

Le suddette prescrizioni (previste dalla normativa privacy a tutela dei dati personali), con particolare riferimento agli obblighi di riservatezza e non divulgazione, si ritengono applicabili a qualsiasi ulteriore informazione di natura tecnica e/o economica propria o di soggetti terzi (es: dati contabili, progetti ed iniziative strategiche, dati tecnici, ecc.) da mantenere, per la loro importanza strategica, in un regime di confidenzialità, in conformità all'Art. 2105 del Codice Civile "dovere di fedeltà".

ART.4: Attivazione e disattivazione utenti informatici

4.1 Attivazione utente L'attivazione dell'utente e del relativo profilo informatico verrà effettuata dagli AdS su indicazione della Direzione o dell'Ufficio incaricato. L'utente è tenuto a rispettare le permission assegnate, evitando qualsiasi tentativo di accesso a risorse non pertinenti con il proprio profilo (le procedure di autenticazione danno automaticamente accesso alle risorse informatiche ed ai dati necessari alle rispettive mansioni personali). L'AdS assegna e revisiona periodicamente le autorizzazioni di accesso alla Rete Informatica al fine di verificarne la congruità con i ruoli ricoperti e provvede tempestivamente alla rimozione dei diritti di accesso al termine del rapporto di lavoro, collaborazione o contrattuale. Le directory di rete possono essere condivise o personali, pertanto si invita gli utenti a prestare la massima attenzione nel caso di salvataggio su unità di rete condivise di dati sensibili o informazioni riservate. Per qualsiasi dubbio o richiesta relativi ai permessi di accesso configurati sugli share di rete è opportuno rivolgersi agli AdS o alla Direzione.

4.2 Disattivazione utente La disattivazione del profilo utente avverrà a seguito dell'interruzione del rapporto lavorativo oppure a seguito di cambi di mansione che non prevedano l'utilizzo di strumenti elettronici. La disattivazione dell'utente e del relativo profilo informatico verrà effettuata dall'AdS su indicazione della Direzione o dell'ufficio incaricato.
In caso di disattivazione del profilo, i dati relativi all'utente (file, posta elettronica, ecc.) verranno conservati, in via separata non direttamente accessibile, per tempi compatibili con le normali esigenze di continuità operativa, di norma 3 mesi per la posta elettronica (o per obblighi legali / contrattuali ed eventuali procedimenti giudiziari). In riferimento alla posta elettronica, in caso di disattivazione di email individualizzata, si procederà all'attivazione di un risponditore automatico che evidenzi indirizzi alternativi a cui rivolgersi. Qualora venisse assegnata una SIM card e relativo numero, in caso di cessazione del rapporto professionale, potranno venire riassegnati ad utenti che subentrano nelle mansioni.

Nell'ambito delle suddette indicazioni, gli utenti (anche disattivati) potranno esercitare tutti i diritti previsti dagli **art.15-21 GDPR** .(diritto di accesso, rettifica, cancellazione, limitazione, portabilità, opposizione).

ART.5: Procedure di autenticazione e protezione strumenti

5.1 Password Il sistema assegna estremi identificativi (costituiti da user-name e password) ad ogni utente abilitato all'utilizzo di strumenti elettronici (password di accesso a windows) e ad applicativi. Le procedure di autenticazione danno automaticamente accesso alle risorse informatiche e ai dati necessari alle rispettive mansioni personali. Ogni utente deve garantire la **segretezza** delle proprie credenziali e la loro **sostituzione periodica**. La password scelta non dovrà avere meno di **8 caratteri** e non dovrà contenere riferimenti diretti a nome/cognome dell'utente. La sostituzione della password potrà essere richiesta automaticamente dai sistemi, tramite impostazione di scadenza automatica.
E' fatto divieto a ciascun utente di divulgare, per fatto imputabile a lui direttamente o indirettamente, password, login e comunque chiavi di accesso riservate. SE smarrite va fatta immediatamente segnalazione al Responsabile di Servizio e richiesta di sostituzione.

In caso di assenza prolungata dell'UTENTE, qualora eventuali circostanze lo rendessero necessario (es: motivi di sicurezza informatica e/o motivi di continuità operativa dell'Ente) le credenziali di autenticazione all'ambiente informatico degli utenti (file, cartelle, database, posta elettronica, ecc.) potranno, su richiesta della Direzione o dell'interessato, essere **resettate dagli AdS**, che provvederanno ad utilizzare il sistema con credenziali provvisorie. In tale caso l'utente provvederà a ripristinare una password segreta al rientro.

5.2 Protezione postazioni **In caso di allontanamento dalla postazione lavorativa, per un periodo prolungato, si richiede di attivare lo screensaver con Password o bloccare il computer (attraverso la combinazione di tasti simbolo "Windows+L" oppure "Ctrl + Alt + Canc" + Blocca computer).**

ART.6: Utilizzo della Posta elettronica

6.1 Premessa L'Ente ritiene che l'uso abituale e corretto della posta elettronica possa migliorare la circolazione delle informazioni e favorire la rapidità delle comunicazioni. La posta elettronica rappresenta pertanto uno strumento idoneo ad agevolare il perseguimento delle finalità dell'Ente, contribuendo inoltre alla riduzione della circolazione della carta e permettendo la facile archiviazione e storicizzazione dei messaggi trasmessi e ricevuti.

6.2 Finalità d'uso La casella di posta elettronica, anche se contenente riferimenti individualizzati, è uno **strumento esclusivamente di lavoro e pertanto deve essere utilizzata per fini lavorativi.** Le persone assegnatarie sono responsabili del corretto utilizzo delle stesse. L'utente è responsabile della segretezza della propria posta elettronica e si impegna a salvaguardare la riservatezza dei propri parametri di accesso, segnalando tempestivamente ogni circostanza che possa comprometterla. L'utente deve prestare particolare attenzione alla sicurezza del dispositivo hardware eventualmente utilizzato per scaricare i messaggi di posta elettronica, soprattutto se si tratta di un dispositivo mobile (notebook, smartphone, tablet, ecc.), maggiormente soggetto a rischio di furto.

6.3 Assegnazione / Revoca L'assegnazione a qualsiasi soggetto di un indirizzo email ufficiale viene effettuata a totale ed autonoma discrezione dell'Ente. E' facoltà dell'Ente disattivare, a suo insindacabile giudizio, le caselle di posta elettronica concesse in utilizzo agli utenti. E' possibile l'assegnazione ed utilizzo (anche condiviso) di caselle email generiche, quali info@..., ecc.

6.4 Supporto tecnico La casella può essere utilizzata in modalità webmail oppure configurata per l'utilizzo attraverso un client di posta. Ogni attività di manutenzione, aggiornamento, implementazione, supporto agli utenti inerente al sistema di gestione della posta elettronica sarà effettuata dagli AdS (al quale è possibile rivolgersi per qualsiasi esigenza di supporto). Tali attività potranno comportare l'accesso ai messaggi di posta inoltrati o ricevuti dagli utenti, esclusivamente in relazione alle suddette finalità e garantendo il rispetto delle vigenti normative internazionali in materia di privacy.

6.5 Regole uso posta elettronica L'utente è responsabile, in via diretta ed esclusiva, dell'attività svolta tramite la propria casella. A tal fine si impegna a:

- utilizzare il servizio di posta elettronica per i soli fini connessi all'attività lavorativa e a essa riconducibili.
- osservare il presente regolamento;
- non arrecare, attraverso l'uso della posta, danni e/o pregiudizi all'Ente, a terzi o ad altri utenti;
- ispirarsi sempre a principi di diligenza, correttezza e buona fede, uniformandosi nei contenuti e nella forma dei messaggi ad adeguati standard di cortesia e buona condotta.
- utilizzare nei messaggi di posta elettronica un linguaggio chiaro, puntuale, rispettoso dell'interlocutore e dei terzi.

L'utente non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, foto, video, audio, ecc.) messaggi che:

- possano danneggiare la reputazione e l'immagine dell'Ente o comprometterne le relazioni con soggetti terzi;
- siano diffamatori, violenti, osceni, offensivi, tali da recare danno o che possano essere considerati fonte di molestie o discriminazione religiosa, sessuale, razziale, politica;

- contengano pubblicità non istituzionale, manifesta, occulta o comunicazioni commerciali private;
- possano infrangere la legislazione vigente, in particolare quella sui diritti d'autore;
- contengano virus e/o altri codici dannosi, o spamming (materiali indesiderati).

Non è consentito, senza una preventiva autorizzazione della Direzione, attivare nuove caselle email con fornitori di servizi di posta elettronica (es: gmail), da utilizzarsi per fini connessi alle attività istituzionali dell'Ente, oltre a quelle già attive e censite con apposito provvedimento del Direttore.

6.6 Destinatari multipli e funzione di inoltro L'invio di messaggi a **destinatari multipli** può comportare la divulgazione non autorizzata di dati riferiti a soggetti terzi, pertanto si richiede, per garantire la privacy dei destinatari, di utilizzare il campo **ccn: C**opia **C**onoscenza **N**ascosta (i campi "a:" o "cc:" comportano che i destinatari possano visualizzare i dati degli altri, pertanto sono da utilizzarsi solo nel caso in cui la condivisione del messaggio sia indispensabile rispetto alla natura del messaggio stesso). **Esempi di invii in cui usare copia nascosta CCN**: invio di auguri, comunicazioni di chiusura, ecc. Si segnala inoltre di prestare la massima attenzione all'utilizzo della funzione **Inoltro**, cancellando le parti che contengono informazioni non riferite al destinatario;

6.7 Firma e risponditore automatico Il sistema prevede l'inserimento automatico nei messaggi in uscita di una firma personalizzata: è vietato modificare i contenuti della firma preimpostata se non preventivamente autorizzati. In caso di assenza prolungata dal posto di lavoro gli utenti possono autonomamente utilizzare la funzione di "risponditore automatico" che indichi il periodo di assenza o le coordinate di un interlocutore alternativo.

6.8 Posta Elettronica Certificata Gli incaricati autorizzati a gestire la Posta Elettronica Certificata (PEC), porranno massima attenzione nell'utilizzo di questo strumento al quale la legge italiana riconosce lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale, garantendone così il non ripudio. E' importante che lo spazio della casella di posta non si saturi: gli incaricati monitoreranno lo spazio disponibile sulla casella e la utilizzeranno solo quando indispensabile. Si raccomanda di prestare le dovute cautele (vedi paragrafo seguente) in merito alla prevenzione di virus e malware anche in relazione all'utilizzo della PEC.

6.9 Posta in arrivo indesiderata (spam) Le caselle di posta elettronica sono dotate, al fine di bloccare in entrata i messaggi ritenuti indesiderati, di un apposito filtro anti-spam, che agisce su 2 livelli:
1) i messaggi riconosciuti come bassa minaccia sono messi in "quarantena", l'utente riceve un avviso e può abilitarli;
2) i messaggi riconosciuti come alta minaccia sono bloccati, pertanto è possibile, in caso si sospetti la mancata ricezione di un messaggio, richiedere all'AdS la verifica della lista delle email bloccate.

LINEE GUIDA E BEST PRACTICE PER L'USO DELLA POSTA ELETTRONICA

Si forniscono alcuni suggerimenti atti ad agevolare il miglior utilizzo del servizio di posta elettronica, in relazione alla composizione/invio dei messaggi ed all'organizzazione della casella.

Suggerimenti per la fase di composizione dei messaggi:

- *inserire sempre l'oggetto del messaggio, espresso in termini chiari e concisi;*
- *evitare nel testo impostazioni, sfondi e strutture complesse che potrebbero arrivare alterati al destinatario;*
- *esprimere in modo professionale e corretto il contenuto del messaggio, possibilmente scrivendo il messaggio direttamente nel campo testo, evitando allegati non necessari;*
- *evitare l'invio e la ridistribuzione di messaggi con allegati superiori a 2 MB, al fine di non sovraccaricare la rete e non saturare le caselle dei destinatari;*
- *utilizzare font standard (preferibilmente Arial o Times New Roman), con grandezza adeguata (da 10 a 12 punti) possibilmente in colore nero ed in carattere minuscolo;*
- *fornire gli estremi identificativi del mittente, inserendo il proprio nome e cognome nel campo testo a fine messaggio.*
- *verificare attentamente il contenuto complessivo prima di spedire, con particolare attenzione all'esattezza degli indirizzi, all'inserimento dell'oggetto ed alla presenza degli allegati;*
- *limitare la diffusione dei messaggi ai destinatari effettivamente interessati;*
- *nell'impostare la priorità usare come criterio l'interesse del destinatario, non del mittente;*
- *limitare l'uso delle ricevute di ricezione/lettura ai casi di effettiva necessità;*
- *limitare l'uso della risposta a tutti dove è sufficiente quella al mittente;*
- *rinviare i messaggi al mittente qualora vengano ricevuti per errore;*
- *non dare per scontata la sollecitudine del destinatario nel leggere la posta o l'infallibilità della tecnologia, contattando direttamente gli interessati qualora non si riceva risposta/ricevuta nei termini attesi.*

Suggerimenti per un'efficiente organizzazione della casella

- *organizzare i messaggi in directory secondo logiche che permettano di reperire con facilità e velocità i messaggi;*
- *cancellare periodicamente i messaggi più datati, assicurando una corretta gestione dello spazio disponibile.*

ART.7: Utilizzo di Internet

Il personal computer abilitato alla navigazione web e qualsiasi connessione ad internet intestata all'Ente costituiscono di norma strumenti da utilizzarsi per funzioni istituzionali o per lo svolgimento dell'attività lavorativa.

7.1 Browser di navigazione L'accesso ad Internet può essere effettuato solamente tramite il browser di navigazione preinstallato. Si richiede di non memorizzare credenziali di accesso nella memoria del browser. Si richiede inoltre di effettuare il log-out al termine dell'utilizzo di applicazioni che prevedono una procedura di autenticazione.

7.2 Filtri automatici Ai fini della sicurezza dei dati trattati e a tutela della propria immagine l'Ente può applicare alla propria rete informatica filtri di accesso (anche differenziati) che impediscono l'accesso ad alcune categorie di siti web il cui elenco viene periodicamente aggiornato e che potrà dunque essere incrementato e/o comunque variato. Per qualsiasi necessità di personalizzazione, anche temporanea, dei filtri sarà necessario rivolgersi alla Direzione.

7.3 Comportamenti vietati Non è consentito:

- effettuare ogni forma di accesso e/o registrazione a siti i cui contenuti non siano strettamente legati all'attività istituzionale/lavorativa;
- l'effettuazione di qualunque genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente previsti dalla mansione o autorizzati dall'Ente;
- l'accesso a siti ancorchè appartenenti alle categorie autorizzate per attività non attinenti alle mansioni assegnate e nell'esercizio delle medesime;
- la partecipazione, per motivi non istituzionali/professionali a «forum», l'utilizzo di «chat line», di bacheche elettroniche e «social network» anche utilizzando pseudonimi (o nicknames);
- il prelevamento e memorizzazione da siti Internet (download) di software gratuiti (freeware) e (shareware), salvo che ciò non sia espressamente autorizzato dall'AdS;
- l'invio (upload) di file e/o dati verso Internet, fatta eccezione per quanto strettamente attinente alla propria attività lavorativa e nell'esercizio autorizzato della medesima;
- la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- Il tentativo di forzare i filtri automatici di cui al punto precedente al fine di accedere a siti non consentiti.

7.4 Utilizzo social network e canali web ASP riconosce che i nuovi canali di comunicazione on-line (principalmente social network) sono strumenti di interazione importanti, con un enorme potenziale; tuttavia, se utilizzati in modo improprio, possono generare diversi profili di rischio, sia personali che lavorativi. La linea di demarcazione tra pubblico e privato, tra personale e professionale, non è mai "assoluta" (spesso il profilo privato è associato a riferimenti istituzionali e viceversa): si suggerisce pertanto un utilizzo dei social equilibrato e rispettoso, uniformato ai principi etici ed ai valori cui l'Ente si ispira. A tal proposito si rinvia a quanto indicato nell'art. 11 ter del vigente Codice di Comportamento dei dipendenti adottato da ASP, riportato nell'Appendice 5
In questa sede si richiama l'attenzione sul fatto che qualsiasi contenuto immesso on-line dall'utente attraverso i propri profili social può essere fonte di responsabilità personale, anche legale.

Si richiede inoltre di segnalare qualsiasi contenuto con cui si venga in contatto nel web che possa arrecare pregiudizio ad ASP Si specifica infine che, nel rispetto delle suddette indicazioni, risulta comunque incentivata l'interazione con le pagine social istituzionali attraverso i propri profili personali.

7.5 Cybersecurity Il numero crescente di cyber crime, ossia di truffe sul web, rende necessaria una grande sensibilità e attenzione da parte degli utenti, al fine di proteggere sé stessi e l'Ente da potenziali rischi. Le aziende sono infatti i bersagli prediletti dai criminali, il cui obiettivo non è solamente trarre un profitto in termini economici, ma anche estrapolare dati critici in possesso dell'impresa. Gli attacchi non avvengono solo tramite gli strumenti di connessione della rete (es. il router), ma anche attraverso i singoli dispositivi come computer e smartphone in uso ai dipendenti. I vettori di attacco possono essere tutte le tecnologie di interconnessione: siti web, posta elettronica, applicazioni di messaggistica (sms, chat, ecc.), portali social, ecc. I criminali informatici utilizzano principalmente i seguenti metodi di attacco nei confronti degli utenti:

- tentativi di "estorcere" alla vittima il maggior numero di informazioni possibile (anche password e codici di accesso) tramite mail / siti / messaggi / chat / profili social verosimili dal punto di vista formale e nella tempistica (tecniche note come phishing);
- tentativi di indurre la vittima a cliccare link o aprire file che contengono codice malevolo, che spesso ha l'effetto di criptare il file e richiedere un riscatto per la decriptazione (tecniche note come ranswomware o cryptolocker);
- tentativi di indurre la vittima ad effettuare operazioni fasulle, simulando l'identità altrui (tecniche note come man in the middle).

Adottando però alcune precauzioni è possibile ridurre notevolmente il rischio di avere il proprio computer infettato o di infettare la rete ed il computer di altri utenti.

- **Si richiede di non aprire e soprattutto non eseguire (non avviare cliccando due volte) file allegati a messaggi di origine incerta o il cui scopo non è chiaro, anche se provenienti da mittenti noti.** Di seguito, sono esposti alcuni indizi che possono scoraggiare l'apertura di messaggi o, soprattutto, l'esecuzione di allegati: indirizzo del mittente non conosciuto, indirizzo del mittente composto da nomi di fantasia o non identificabili, mancanza dell'oggetto, testo del messaggio fuori contesto o con informazioni non richieste, utilizzo di caratteri non decifrabili, utilizzo di lingue straniere fuori contesto, contenuto del messaggio offensivo, contenuto del messaggio a carattere sessuale, contenuto del messaggio con lusinghe fuori contesto. In ogni caso non dovrebbero mai essere avviati file allegati che abbiano estensioni tipo .exe, .scr,.vbs,.bat,.com
- **E' buona prassi, prima di cliccare link contenuti in email o siti, verificare:**
- la corrispondenza tra il link visualizzato in corso testo e quello che compare, posizionando il cursore del mouse sul link stesso, nella barra di stato;
- in caso di apertura della pagina, la corrispondenza del link visualizzato in corso testo e quello che compare nella barra di indirizzo del browser di navigazione.
- Di norma evitare di inviare via email / divulgare dati sensibili/riservati o credenziali di accesso (in caso di necessità privilegiare l'invio di allegati in formato zip protetto da password; con firma digitale; tramite PEC).
- Prima di effettuare operazioni finanziarie occasionali o modifiche di dati finanziari (es: modificare l'iban di un fornitore dietro richiesta via email): verificare sempre, preferibilmente tramite contatto telefonico diretto, l'identità del richiedente e la veridicità della richiesta. Nel caso di cambio IBAN fornitori oltre alla verifica, tramite contatti diretti, seguire la procedura per la tracciabilità dei flussi finanziari.
- Effettuare, al termine dell'uso, il log-out da portali che richiedono l'accesso tramite autenticazione.
- Verificare se il sito web utilizza protocolli di sicurezza (https) e prestare attenzione ad eventuali suggerimenti del browser di navigazione.

Di prassi è dunque sempre preferibile un approccio cauto, diffidando di tutto ciò che non è semplice testo (principalmente link ed allegati) evitandone, in caso di dubbio, l'apertura.

ART.9: Ulteriori apparati e strumenti

9.1 Notebook Ai computer portatili si applicano le regole di utilizzo previste per i PC di cui sopra. Si raccomanda una maggior attenzione per la criticità insita nello strumento informatico in oggetto. I PC portatili utilizzati all'esterno, quando non vengono utilizzati, devono essere custoditi in un luogo protetto per prevenirne il furto.

9.2 Mobile device (smartphone, tablet) Anche all'utilizzo dei mobile device si applicano le medesime prescrizioni del presente Regolamento. In relazione alle peculiarità degli strumenti mobile si ritiene opportuno sottolineare le seguenti prescrizioni (atte a garantire un corretto utilizzo dello strumento ed un adeguato livello di protezione dei dati):

- non modificare le impostazioni dello strumento, con particolare riferimento all'installazione/disinstallazione di applicazioni;
- segnalare immediatamente eventuali anomalie o malfunzionamenti;
- prestare particolare attenzione alla custodia dello strumento, evitando di lasciarlo incustodito e segnalando immediatamente l'eventuale smarrimento/furto;
- non consentire l'utilizzo o l'accesso ai dati a soggetti non autorizzati (prestando particolare attenzione all'utilizzo dello strumento in luoghi pubblici);
- evitare di collegare lo strumento a dispositivi non istituzionali.

Al fine di limitare i suddetti rischi, ASP si riserva di utilizzare/richiedere apposite funzionalità tra cui:

- attivazione PIN della SIM Card
- attivazione di ulteriori procedure di autenticazione (ad applicazioni o supporti di memoria)
- impostazione di prestabiliti tempi di session time-out
- attivazione delle procedure di remote-wiping da utilizzare in caso di smarrimento/furto del dispositivo
- attivazione delle funzionalità di cifratura automatica dei dati
- sistemi di controllo delle applicazioni installabili (c.d. white list)
- sistemi di blocco navigazione e tracciatura attività
- sistemi di geolocalizzazione in caso di smarrimento/furto

9.3 Chiavette USB In generale è vietato l'utilizzo di sistemi di personal storage o di supporti rimovibili personali se non autorizzati espressamente. L'utilizzo di supporti rimovibili o personal storage deve essere assegnato ed autorizzato da ASP e disciplinato dagli AdS. Gli utenti sono pertanto tenuti, in caso di necessità, a richiedere l'utilizzo di tali strumenti.
In generale le unità di memoria esterne devono prevedere il blocco di funzioni di auto-esecuzione e la cifratura dei dati.

9.4 Stampanti e fax Le stampe dimenticate possono spesso costituire involontaria fuga di notizie. Si raccomanda quindi la massima attenzione nell'utilizzo delle stampanti, con particolare riferimento alla corretta distruzione di documenti che non servono più. E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. E' necessario prestare la massima attenzione all'eventuale riutilizzo di stampe (carta

da riciclo): tale pratica è di norma autorizzata solo quando i documenti contengano dati non personali pubblici. Il servizio Fax è considerato, per motivi organizzativi, una componente del circuito di comunicazione e quindi viene trattato con le stesse regole di un qualsiasi documento.

9.5 Strumenti hw specifici (token, card, ecc.) Gli strumenti hardware necessari all'effettuazione di specifiche operazioni (dispositivi e card per la firma digitale, token per operazioni bancarie, carte di credito, ecc.) devono essere utilizzati esclusivamente dagli utenti espressamente identificati ed autorizzati. Tali utenti sono responsabili del corretto utilizzo di tali strumenti e devono preoccuparsi di:

- non consentirne l'accesso e l'utilizzo a soggetti non autorizzati;
- riporli alla fine dell'utilizzo (che deve essere il più possibile limitato nel tempo) nella posizione idonea;
- adottare tutti gli accorgimenti atti a prevenirne il furto o lo smarrimento.

Rientrano nelle medesime prescrizioni gli strumenti di registrazione degli accessi e delle presenze.

9.6 Scanner Gli strumenti preposti alle scannerizzazioni di documenti consentono all'utente di selezionare la destinazione del file che viene generato (email o directory di rete). E' cura degli utenti selezionare la destinazione corretta e rimuovere il documento cartaceo originario dall'apparato. Qualora i dispositivi memorizzino le scansioni in directory comuni, è necessario spostare prontamente il file, mediante funzione taglia/incolla.

9.7 Accesso tramite VPN e smartworking E' facoltà dell'Ente autorizzare e configurare la possibilità di collegamento da remoto con la LAN tramite tecnologie di connessione, di seguito indicate complessivamente, per semplicità, VPN (rendendo possibile la pratica di smartworking o telelavoro). L'utente si impegna a rispettare le seguenti prescrizioni:

- il collegamento VPN (configurandosi quale strumento di lavoro idoneo ad abilitare l'accesso da remoto a sistemi dell'Ente) deve essere utilizzato a soli scopi lavorativi, nel rispetto delle regole e delle istruzioni in materia di trattamento dei dati personali;
- in caso di utilizzo di uno strumento di proprietà dell'Ente è necessario non alterarne le configurazioni di sistema e di sicurezza;
- in caso di utilizzo di uno strumento proprio personale è necessario che esso sia dotato di requisiti minimi di sicurezza, quali accesso con password, antivirus, firewall e sistema operativo aggiornato;
- l'utilizzo della VPN è ad uso esclusivo dell'utente abilitato (che deve garantire la segretezza delle credenziali di accesso) e nei limiti della prestazione lavorativa assegnata;
- l'utente deve prevenire qualsiasi accesso indebito al sistema, avendo cura delle potenziali situazioni di promiscuità dell'ambiente lavorativo / domestico, bloccando la postazione in caso di allontanamento.

9.8 Tecnologie di videoconferenza L'utilizzo di tecnologie di videoconferenza deve avvenire nel rispetto delle indicazioni del presente regolamento, al fine di agevolare i contatti professionali:

- non è consentita la registrazione delle videochiamata, se non preventivamente autorizzato da tutti i partecipanti;
- ogni immagine immessa dall'utente tramite la propria webcam è di esclusiva responsabilità dell'utente stesso.

9.9 Reti WI-FI L' utilizzo delle **reti wi-fi** istituzionali potrà avvenire esclusivamente nel rispetto delle regole identificate nel presente documento e di eventuali ulteriori policy codificate da ASP. E' facoltà dell'AdS configurare diverse reti wi-fi, impostando adeguati parametri di accesso, in relazione alle esigenze operative ed ai requisiti di sicurezza. In generale potranno essere previste specifiche policy per il corretto utilizzo delle reti wifi locali.

9.10 Strumenti personali L'Ente si riserva la possibilità di approfondire la regolamentazione (in relazione al progresso tecnologico ed alle necessità degli utenti) dell'utilizzo di strumenti personali nel contesto istituzionale. Al momento, se non espressamente autorizzati, è da ritenersi vietato:

- la memorizzazione di dati relativi all'attività dell'Ente su dispositivi personali;
- utilizzare / connettere alle reti istituzionali dispositivi personali;
- l'uso di caselle di posta personali ed applicazioni, non espressamente autorizzate, per fini lavorativi;

In caso di autorizzazione all'utilizzo di strumenti personali per attività lavorativa, l'utente si impegna ad utilizzare strumenti che garantiscano un adeguato livello di sicurezza (es: accesso con password, antivirus, firewall e sistema operativo aggiornato, ecc.).

Durante l'orario di lavoro è consentito l'uso del cellulare personale, per fini personali, solamente in casi di comprovata urgenza e necessità, comunque in modo occasionale, limitato nel tempo e non interferente con l'attività lavorativa propria ed altrui. L'Ente si riserva la possibilità, escludendo qualsiasi forma di raccolta / archiviazione di dati personali, di richiedere all'utente l'utilizzo di proprio strumento personale per l'installazione di app connesse a modalità sicure di autenticazione (Multi Factor Authentication), al fine di migliorare la postura di sicurezza e le procedure di accesso ai dati.

9.11 Intelligenza artificiale Gli utenti presteranno la dovuta attenzione all'utilizzo degli strumenti di intelligenza artificiale, tra quelli liberamente disponibili on-line o integrati in applicativi in uso all'Ente). A meno di espresse autorizzazioni, non è consentito caricare su strumenti di intelligenza artificiale informazioni rilevanti / riservate / personali. In generale è

necessario l'utilizzo dell'intelligenza artificiale nel rispetto dei divieti sanciti dall'AI Act (Regolamento (UE) 2024/1689): manipolazione cognitivo comportamentale; sfruttamento di vulnerabilità; social scoring; riconoscimento/sorveglianza biometrica.

9.12 Documenti cartacei e colloqui Tutti i documenti cartacei devono essere gestiti in modo da **ridurre al minimo** i tempi di permanenza al di fuori degli archivi (per archivi si intende a titolo esemplificativo: armadi, contenitori, faldoni, classificatori, fascicoli, ecc. in dotazione alle unità operative). Massima attenzione dovrà essere posta per i documenti che si trovano in locali accessibili al pubblico. L'accesso agli archivi è consentito al personale a ciò espressamente autorizzato in via permanente od occasionale. Gli archivi devono essere mantenuti costantemente chiusi/controllati, compatibilmente con le esigenze di servizio. Le copie dei documenti vanno trattate, con riferimento alla tutela dei dati personali in esse contenuti, con la medesima diligenza riservata agli originali. Gli utenti sono tenuti a vigilare sull'accesso ai locali in cui operano da parte di personale non identificato o non autorizzato. A tale proposito si raccomanda una gestione ordinata delle proprie scrivanie e spazi di lavoro, limitando il possibile accesso alle informazioni ivi conservate a persone non autorizzate. A fine giornata lavorativa o in caso di prolungata assenza dalla postazione si richiede di riordinare le proprie scrivanie, riponendo i documenti negli appositi archivi. Evitare di lasciare documenti in aree adibite al ricevimento di persone, quali reception / locali adibiti a riunione (in cui, al termine delle attività, occorre prestare attenzione anche ad eventuali dati rimasti scritti su lavagne/espositori). Si raccomanda infine particolare attenzione al tono di voce ed alla situazione di riservatezza anche per eventuali **colloqui e conversazioni con contenuti riservati**, in quanto anche l'ascolto di tali informazioni potrebbe dar luogo ad utilizzi indebiti.

ART.10: Apparati a tutela della sicurezza e disponibilità dei dati

10.1 Back-up Il sistema informatico garantisce attività periodica di back-up per tutti i dati salvati negli appositi spazi sui server. Si richiede pertanto di non archiviare documenti rilevanti negli spazi di memoria dei singoli computer, sui quali non è garantita alcuna attività di back-up.

10.2 Antivirus Il sistema informatico è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, nonché segnalare prontamente l'accaduto. Anche nel caso in cui l'utente rilevi un comportamento anomalo dei propri strumenti informatici (non segnalato dall'antivirus), lo stesso dovrà immediatamente sospendere ogni elaborazione in corso, nonché segnalare prontamente l'accaduto.

10.3 Ulteriori comunicazioni da effettuare Gli utenti sono tenuti a segnalare tempestivamente alla Direzione, anche tramite il proprio Responsabile di Area/Servizio/Unità Operativa::

- qualsiasi evento che possa compromettere la sicurezza e la riservatezza dei dati (definito anche "data breach") tra cui si cita a titolo esemplificativo non esaustivo un attacco informatico, un errore nella gestione/invio dei dati, il furto / smarrimento di dispositivi contenenti dati, ecc.);
- qualsiasi richiesta di esercizio dei diritti degli interessati (GDPR, Art.15-21 "diritti di accesso, rettifica, cancellazione, limitazione, portabilità, opposizione) che dovesse essere loro rivolta da qualsivoglia soggetto;
- qualsiasi richiesta di chiarimento o informazione aggiuntiva in materia di privacy o data protection, che dovesse essere loro rivolta da qualsivoglia soggetto

ART.11: Archiviazione di parametri e dati di utilizzo

11.1 Tecnologie di archiviazione dati Si segnala agli utenti che gli strumenti di rete possono memorizzare temporaneamente le informazioni relative all'uso degli strumenti stessi da parte degli utenti per le seguenti finalità:
- protezione dell'intera rete da e verso l'esterno (firewall, web-blocker, spam-blocker);
- più efficiente utilizzo del collegamento Internet (proxy server);
- difesa della corrispondenza e navigazione informatica (content filtering; web filtering; mail monitoring).

11.2 Conservazione ed accesso ai dati Tutti i dati archiviati nell'infrastruttura tecnologica sono conservati per tempi compatibili e pertinenti con la finalità della raccolta e della registrazione, generalmente commisurata ad esigenze operative, tecniche e di sicurezza (identificati in 6 mesi per i log di navigazione). Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'**esercizio o alla difesa di un diritto** in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una **specifica richiesta dell'autorità giudiziaria**.

I dati memorizzati dagli strumenti non sono costantemente monitorati: l'accesso agli stessi può avvenire esclusivamente secondo le modalità di cui al seguente articolo.

ART.12: Controlli

12.1 Finalità dei controlli Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Ente accedere direttamente (o tramite specifici incaricati, vedi art.2), nel rispetto della normativa sulla privacy, a tutti gli STRUMENTI INFORMATICI e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico o internet.

12.2 Modalità dei controlli Nell'attività di verifica sarà osservato il **principio di gradualità**, operando, qualora possibile controlli su dati aggregati. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati. Resta fermo il diritto del datore di lavoro di effettuare controlli identificativi quando ciò sia dettato da:

- riscontri di mancato rispetto del presente regolamento;
- oggettivi indizi di commissione di reato;
- esigenze di salvaguardia della vita o dell'incolumità di terzi;
- norme specifiche di leggi o dall'autorità giudiziaria;
- specifiche richieste delle forze dell'ordine.

Si elencano inoltre a titolo esemplificativo e non esaustivo alcune circostanze concrete che potrebbero portare a verifiche, anche indirette, dell'ambiente informatico degli utenti:

- sovradimensionamento dei file di back-up;
- malfunzionamento frequente degli strumenti elettronici assegnati;
- segnalazione di circostanze sospette da parte della struttura di protezione della rete e di connettività;
- evidenze o segnalazioni di violazioni o comportamenti non corretti.

In caso di sospetti/evidenze di reato, gli strumenti elettronici potranno essere sottoposti a controllo, anche mediante tecniche di digital forensics, consistenti di norma in: sequestro; forensics imaging (acquisizione di un "immagine" del device, da potersi utilizzare quale elemento probatorio); analisi e relazioni.

ART.13: Obblighi Violazioni e sanzioni

Gli utenti sono tenuti:

- al rispetto del presente Regolamento e di eventuali ulteriori policy emanate in materia di privacy e sicurezza informatica;
- a partecipare alle iniziative di formazione organizzate in materia da Asp.

La violazione degli obblighi previsti dal presente Regolamento integra comportamenti contrari ai doveri d'ufficio previsti dalla legge, dai regolamenti e dai contratti collettivi. Essa è fonte di responsabilità disciplinare, accertata all'esito del procedimento disciplinare, nel rispetto dei principi di gradualità e proporzionalità delle sanzioni.

13.1 Responsabilità dell'utente L'attivazione del procedimento disciplinare e l'irrogazione di una sanzione disciplinare non preclude, né pregiudica l'azione giudiziaria del datore di lavoro:

- di denuncia di atti illeciti di rilevanza penale;
- di risarcimento civile per danni al patrimonio o all'immagine dell'Ente o di soggetti terzi.

Comportamenti scorretti potrebbero generare inoltre in capo al lavoratore:

- responsabilità contrattuale nei confronti del datore di lavoro;
- responsabilità amministrativa e penale in relazione ad eventuali violazioni di vigenti normative (es: privacy, diritto d'autore, copyright, pirateria informatica, ecc.);
- responsabilità civile nei confronti di soggetti terzi che venissero danneggiati in qualsiasi modo da condotte illecite dell'utente.

ART.14: Aggiornamento e revisione

14.1 Comunicazione modifiche Qualsiasi variazione del presente regolamento sarà portata a conoscenza degli utenti secondo opportune modalità. Tutti gli utenti possono rivolgersi alla Direzione e/o Responsabile di Area/Servizio/Unità Operativa per qualsiasi dubbio o richiesta di chiarimento, nonché per proporre, quando ritenuto necessario, integrazioni/modifiche motivate al presente Regolamento.

APPENDICE 1: Indicazioni di sintesi per la prevenzione di reati informatici

E' vietato porre in essere i comportamenti rientranti nel novero dei reati presupposto, in materia di reati informatici, ovvero:

- accedere abusivamente in un sistema informatico o telematico;
- intercettare dati informatici durante trasmissioni non pubbliche**;**
- installare o usare apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- danneggiare informazioni, dati e programmi informatici utilizzati da enti pubblici che intrattengono rapporti con l'Ente o comunque di pubblica utilità;
- danneggiare sistemi informatici o telematici, anche di pubblica utilità;
- detenere e diffondere abusivamente codici di accesso a sistemi informatici o telematici altrui protetto da misure di sicurezza, nonché la semplice diffusione di informazioni finalizzate al medesimo scopo;
- diffondere programmi diretti a danneggiare o interrompere un sistema informatico o telematico;
- tutte le ipotesi di falsità aventi ad oggetto un documento informatico.

APPENDICE 2: Indicazioni di sintesi per la prevenzione di violazioni del diritto d'autore

E' vietato porre in essere i comportamenti rientranti nel novero dei reati presupposto, in materia di violazione del diritto d'autore, in particolare, a solo titolo esemplificativo e non esaustivo:

- mettere a disposizione del pubblico, immettendola in un sistema di reti telematiche mediante connessioni di qualsiasi genere un'opera di ingegno protetta o parte di essa;
- duplicare abusivamente programmi per elaborare o distribuire, vendere, detenere, programmi contenuti in supporti non contrassegnati da marchi;
- duplicare, riprodurre, trasmettere o diffondere in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive;
- abusivamente riprodurre, trasmettere o diffondere in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati.

APPENDICE 3: Modifiche introdotte dal Jobs Act alla Legge 300/70

Art. 23 – D.Lgs.151/2015 (pubblicato in G.U. N° 221 del 23/09/2015) "Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196"

1. L'articolo 4 della legge 20 maggio 1970, n. 300 è sostituito dal seguente: «Art. 4 (Impianti audiovisivi e altri strumenti di controllo). 1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.

2. La disposizione di cui al comma 1 ***non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze****.*

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a ***tutti i fini connessi al rapporto di lavoro*** *a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.»*

Il presente regolamento rappresenta pertanto un'adeguata informazione sulle modalità d'uso e di effettuazione dei controlli sugli strumenti informatici (strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa).

APPENDICE 4: Informativa sul trattamento dei dati (ex. Art. 13 – REG.UE 2016/679)

Relativa ai dati contenuti negli strumenti elettronici, a completamento dell'informativa generale fornita al personale

I dati contenuti e gestiti tramite gli strumenti elettronici possono costituire informazioni classificate quali dati personali relativi agli utenti (def utenti e strumenti, vedi premesse). Tali dati sono trattati esclusivamente al fine di garantire il corretto funzionamento dell'infrastruttura tecnologica, nonchè un adeguato livello di protezione e sicurezza della stessa (finalità coerenti con quelle del presente regolamento, vedi premesse). I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati archiviati (vedi art.12). Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati. Ai dati possono accedere solamente i soggetti di cui all'Art.2, dei quali gli interessati possono liberamente chiedere gli estremi identificativi. I dati non saranno oggetto di diffusione. I dati non sono conferiti dall'interessato, bensì acquisiti direttamente dagli apparati tecnologici e sono trattati in relazione ad un legittimo interesse di operatività e sicurezza del Titolare del trattamento. Gli interessati, contattando la Direzione, hanno facoltà di esercitare tutti i diritti previsti dagli art.15-21 del GDPR:

- diritto di richiedere la presenza e l'accesso a dati personali che la riguardano (Art.15 "Diritto di accesso")
- diritto di ottenere la rettifica/integrazione di dati inesatti o incompleti (Art.16 "Diritto di rettifica")
- diritto di ottenere, se sussistono giustificati motivi, la cancellazione dei dati (Art.17 "Diritto alla cancellazione")
- diritto di ottenere la limitazione del trattamento (Art.18 "Diritto alla limitazione")
- diritto di ricevere in formato strutturato i dati che la riguardano (Art.20 "Diritto alla portabilità)
- diritto di opporsi al trattamento ed a processi decisionali automatizzati, compresa la profilazione (Art.21, 22)
- diritto di revocare un consenso precedentemente prestato;
- diritto di presentare, in caso di mancato riscontro, un reclamo all'Autorità Garante per la protezione dei dati.

APPENDICE 5: Estratto codice di Comportamento di ASP con riferimento all'utilizzo dei mezzi di informazione e social media

Art. 11 ter – Utilizzo dei mezzi di informazione e dei social media

1. I rapporti con i mezzi di informazione sugli argomenti istituzionali sono tenuti dagli organi e uffici deputati dall'Azienda, nonché dai dipendenti espressamente incaricati. L'orientamento dell'Azienda sulle materie di competenza è espresso mediante comunicati ufficiali o dichiarazioni dei suoi organi.
2. Il dipendente, salvo il diritto di esprimere valutazioni o diffondere informazioni a tutela dei diritti sindacali:
   a) evita ogni dichiarazione pubblica concernente la propria attività di servizio;
   b) si astiene da qualsiasi altra dichiarazione che possa nuocere al prestigio ed all'immagine dell'Azienda;
   c) non intrattiene rapporti con i mezzi di informazione in merito alle attività istituzionali;
   d) non sollecita la divulgazione, in qualunque forma, di notizie inerenti all'attività dell'Azienda;
   e) informa tempestivamente l'Azienda per il tramite del proprio Responsabile, nel caso in cui sia destinatario di richieste di informazione o chiarimenti da parte di organi di informazione;
   f) nell'uso dei social network ha specialmente cura di evitare la spendita anche indiretta o implicita del ruolo svolto all'interno dell'Azienda, salvaguardando l'immagine e la credibilità della funzione.
3. Il comportamento del dipendente pubblico deve essere improntato alla correttezza verso l'Azienda, anche al di fuori del luogo e dell'orario di lavoro.
4. Nell'uso dei social network il dipendente deve comportarsi correttamente in modo da non ledere l'immagine di sé come dipendente pubblico, né l'immagine dell'azienda: in particolare non rende pubblici informazioni, foto, video, audio inerenti l'attività lavorativa che possano ledere l'immagine dell'Azienda, l'onorabilità dei colleghi, la riservatezza e la dignità della persona o che violino il segreto d'ufficio.
5. Il dipendente utilizza gli account privati dei social media di cui è titolare in modo che le opinioni, ivi espresse e i contenuti, ivi pubblicati non siano in alcun modo attribuibili direttamente all'Azienda.
6. In ogni caso il dipendente si astiene da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro e all'immagine dell'Azienda o della pubblica amministrazione in generale.
7. Il dipendente osserva anche sui social network il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali. E' vietato divulgare o diffondere per ragioni estranee al proprio rapporto di lavoro documenti, anche istruttori, di cui si ha la disponibilità.
8. E' consentito condividere sulla propria pagina personale i contenuti pubblicati sui social media istituzionali al fine di promuovere un'iniziativa o un'attività dell'Azienda.
9. E' fatto divieto di creare, senza autorizzazione, sui social networks gruppi pagine, profili o simili riconducibili o riferibili all'Azienda.
10. 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 a un'esigenza di carattere istituzionale.