Regolamento
sull'utilizzo di alcuni strumenti aziendali

Premessa e riferimenti normativi

La progressiva diffusione delle nuove tecnologie informatiche, in particolare, il libero accesso alla rete Internet dai Personal Computer aziendali, e l'uso degli strumenti informatici aziendali espongono APS Holding SpA a rischi di natura patrimoniale, oltre che a responsabilità penali conseguenti la violazione di specifiche disposizioni di legge (fra tutte, legge sul diritto d'autore e legge sulla privacy), con conseguenti ripercussioni sulla sicurezza e sull'immagine dell'Azienda stessa.

Per strumenti informatici s'intende l'insieme delle risorse informatiche di APS Holding SpA, ovvero le risorse infrastrutturali e dal patrimonio informativo digitale. Le risorse infrastrutturali sono costituite dalle componenti hardware e software, mentre il patrimonio informativo è l'insieme delle banche dati in formato digitale, nonché di tutti i documenti, anche cartacei, prodotti tramite l'utilizzo delle risorse infrastrutturali o comunque disponibili nelle sedi aziendali.

Per evitare che comportamenti, anche inconsapevoli, dei lavoratori possano minacciare e/o compromettere la sicurezza nel trattamento dei dati, ovvero comportamenti scorretti distolgano le risorse aziendali dall'uso cui le stesse sono deputate, APS Holding SpA ha adotta il presente Regolamento.

Allo scopo di prevenire tali rischi, il presente Regolamento fornisce disposizioni in merito all'utilizzo degli strumenti di natura tecnologica e dei sistemi informatici, con riferimento alle **misure di sicurezza** e dei **comportamenti** che devono essere adottati da parte di coloro che operano per conto d4ella nostra Azienda a tutela delle informazioni gestite per il tramite di strumenti informatici.

La Società ha predisposto la presente Policy in conformità:

- al Regolamento Europeo in materia di protezione dei dati personali 679/2016/EU (c.d. "GDPR");
- al Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007 "Linee guida del Garante per posta elettronica ed Internet" e successivi provvedimenti, tra cui il provvedimento "Accesso alla posta elettronica dei dipendenti" del 22 dicembre 2016".
- all'art. 4 § 2 della Legge n. 300/1970;

Definizione e campo di applicazione

L'azienda APS Holding SpA è il **Titolare** dei trattamenti da essa controllati sui cui ha quindi la responsabilità e l'obbligo di applicare misure tecniche ed organizzative adeguate alla protezione sia dei dati personali trattati che del proprio patrimonio informativo.

Gli **Incaricati** sono tutte le persone fisiche che sono incaricate della Società di effettuare trattamenti informatici ed utilizzano a questo scopo strumenti Società. In questa categoria sono

APS Holding S.p.A.
Società soggetta all'attività di direzione
e coordinamento del Comune di Padova
Società a Socio Unico

Via Salboro 22/b - 35121 Padova | T. +39 049 5660111 - F. +39 049 5660112
E. info@apsholding.it | PEC apsholding@legalmail.it | www.apsholding.it
C.F./P.IVA 03860240286 | REA PD 342892 | Cap. sociale i.v. € 49.508.016

quindi compresi i dipendenti senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori coordinati e continuativi, in stage, ecc.).

Il presente Regolamento si applica pertanto a tutti gli Incaricati (o utenti), come sopra descritti.

Il rispetto del presente regolamento è un prerequisito per l'utilizzo delle attrezzature informatiche aziendali e degli applicativi che permettono l'utilizzo delle risorse informative aziendali. La consequente raccolta, da parte del Titolare, dei dati generati dall'uso di tali attrezzature e software ivi installati, è necessaria per consentire all'Utente di fruire degli strumenti tecnologici di proprietà o nella disponibilità aziendale.

Considerazioni generali

Ciascun dipendente si impegna a garantire la **massima riservatezza** riguardo a tutte le informazioni di cui viene a conoscenza nel corso del proprio lavoro evitando la divulgazione e la copia anche accidentali dei dati.

Inoltre, l'azienda APS Holding SpA è esclusiva titolare e proprietaria dei dispositivi messi a disposizione degli Incaricati ai soli fini dell'attività lavorativa, ed è **l'unica esclusiva titolare e proprietaria** di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati con i propri dispositivi o archiviati in modo cartaceo nei propri locali.

Inoltre, gli strumenti aziendali sono forniti ai dipendenti e collaboratori a discrezione dell'azienda, allo scopo di promuovere l'efficacia e l'efficienza della medesima e conseguire gli obiettivi di business di APS Holding SpA.

Pertanto, il dipendente non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi aziendali siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'azienda.

Di conseguenza, l'Azienda avrà diritto di accedere a tali strumenti aziendali (incluso l'account di posta elettronica e ai messaggi ricevuti e trasmessi tramite lo stesso) in caso di assenza o impedimento dei dipendenti e/o per la manutenzione periodica degli Strumenti Aziendali, al fine di assicurare la continuità delle attività aziendali, la sicurezza dei sistemi e il loro corretto funzionamento, nonché l'integrità dei dati.

Ciascun dipendente, nell'esecuzione delle attività quotidiane, deve:

- gestire le proprie password secondo le regole descritte di seguito;
- ridurre al minimo le copie di lavoro distruggendo le copie cartacee quando non più necessarie;
- attuare una politica di "scrivania pulita" per i documenti ed i supporti di memorizzazione rimovibili, sia una politica di "schermo pulito" per i servizi di elaborazione delle informazioni. In particolare, si richiede di bloccare l'accesso alla postazione ogni qualvolta la si lascia incustodita.

APS Holding S.p.A.
Società soggetta all'attività di direzione
e coordinamento del Comune di Padova
Società a Socio Unico

Via Salboro 22/b - 35124 Padova | T. +39 049 5660111 - F. +39 049 5660112
E. info@apsholding.it | PEC apsholding@legalmail.it | www.apsholding.it
C.F./P.IVA 03860240286 | REA PD 342892 | Cap. sociale i.v. € 49.508.016

Per la medesima ragione al **termine del rapporto di lavoro**, tutti i dispositivi aziendali e le copie cartacee dei dati devono essere restituite. Eventuali copie elettroniche dei dati in possesso del collaboratore vanno cancellate.

Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970; conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al successivo punto 14), termo restando il rispetto della normativa in materia di protezione dei dati personali (D.lgs. n.196/2003 e s.m.i. e reg EU 679/2016).

Istruzioni per gli Incaricati

Riguardo all'utilizzo di PC e dispositivi aziendali assegnati personalmente

Il personal computer ed il telefono Smartphone affidato all'Incaricato sono strumenti di lavoro.

Vengono messi a disposizione dell'Incaricato in relazione al ruolo svolto all'interno della Società, previa approvazione da parte della Direzione. L'Incaricato deve custodirli ed utilizzarli con la massima diligenza rispetto allo strumento e alla gestione del traffico telefonico e dati.

L'uso del telefono aziendale per l'effettuazione di telefonate personali o comunque non strettamente inerenti l'attività lavorativa stessa è consentito solo nel caso di comprovata necessità ed urgenza.

I Gestori telefonici inviano periodicamente all'azienda una distinta del traffico telefonico effettuato dagli Utenti con i numeri di destinazione parzialmente oscurati; l'Azienda si riserva la facoltà di addebitare all'Utente importi derivanti da telefonate personali in quantità giudicate superiori ad un normale utilizzo.

L'Azienda si riserva il diritto di chiedere in qualsiasi momento la restituzione dei Dispositivi Mobili aziendali e delle schede SIM.

Ogni Utente è chiamato a fornire il proprio contributo al fine di minimizzare la possibilità che i dati aziendali che eccezionalmente e solo temporaneamente possono essere contenuti in telefoni cellulari, smartphone e tablet siano esposti a rischi di sicurezza.

Si raccomanda la massima attenzione nel non lasciare incustoditi telefoni cellulari, smartphone e tablet.

Devono essere rispettate le seguenti regole:

a) Non è consentita l'installazione e l'uso di programmi provenienti dall'esterno, senza la preventiva autorizzazione scritta del Responsabile dei Sistemi informativi. Tutti i programmi

APS Holding S.p.A.
Società soggetta all'attività di direzione
e coordinamento del Comune di Padova
Società a Socio Unico

Via Salboro 22/b - 35121 Padova | T. +39 049 5660111 - F. +39 049 5660112
E. info@apsholding.it | PEC apsholding@legalmail.it | www.apsholding.it
C.F./P.IVA 03860240286 | REA PD 342892 | Cap. sociale i.v. € 49.508.016

installati devono avere regolare licenza d'uso. In particolare è vietato installare ed utilizzare soluzioni cloud (come ad esempio weTransfer, Dropbox, Google Drive, ecc.);

L'inosservanza della presente disposizione espone la nostra azienda a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziati vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico di APS Holding SpA, come disposta dall'art. 25-nonies del Dlgs. 8 giugno 2001 n. 231 con conseguente applicazione di sanzioni pecuniarie ed interdittive.

b) È vietato disabilitare, disinstallare, modificare o rendere in tutto o in parte inservibili programmi, informazioni o dati aziendali, nonché modificare in tutto o in parte i software o le loro configurazioni di funzionamento; in particolare è vietato disattivare, anche temporaneamente, il sistema antivirus ed altri software di protezione logica presenti sui dispositivi;

c) È vietato disabilitare e modificare le impostazioni di sicurezza dei dispositivi, per esempio disattivare, anche temporaneamente, il PIN della SIM card, disattivare il salvaschermo, disattivare l'antivirus, violare l'integrità del sistema operativo (jailbreak o modding) ed altre misure analoghe;

d) Il Personal Computer deve essere spento ogni sera, prima di lasciare gli uffici, nonché in caso di assenze prolungate dall'ufficio e in caso di suo inutilizzo;

e) Nel caso in cui il software Antivirus rilevi la presenza di virus, l'utente deve immediatamente segnalarlo agli incaricati dei Sistemi informativi.

f) L'installazione e l'uso di dispositivi di comunicazione o memorizzazione (modem, chiavette, masterizzatori, ...), è consentito solo per dispositivi di proprietà aziendale e previa autorizzazione scritta del Responsabile dei Sistemi informativi;

g) eventuali comportamenti anomali dello strumento, notifiche o allarmi inerenti alla sicurezza del dispositivo devono essere prontamente segnalate al personale dei Sistemi informativi;

h) qualora questo il proprio dispositivo personale fosse rubato o smarrito, è necessario:

   1. segnalare prontamente lo smarrimento al reparto Sistemi Informativi;
   2. modificare prontamente tutte le password memorizzate sul dispositivo.

i) I supporti rimovibili che contengono dati (di qualunque tipo: personali, identificativi, particolari, ma anche di tipo aziendale o industriale come disegni, progetti, documenti, ...) devono essere custoditi in archivi chiusi a chiave;

j) Il personale dei Sistemi informativi ha la facoltà di verificare periodicamente tutta la Rete Aziendale procedendo, se necessario, anche alla rimozione immediata di eventuali software installati senza licenza o comunque non autorizzati.

NB per autorizzazione scritta si intende anche una comunicazione di posta elettronica.

Alla cessazione del rapporto di lavoro, gli strumenti aziendali devono essere prontamente restituiti alla Società nello stesso stato in cui sono stati consegnati, fatto salvo il normale degrado d'uso.

Riguardo all'utilizzo di altri dispositivi

È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di Area/ Funzione.

È vietato l'utilizzo delle fotocopiatrici e stampanti aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Area/Funzione

Riguardo all'utilizzo di PC e dispositivi personali e privati

L'azienda favorisce l'uso di dispositivi personali per accedere ad alcune applicazioni aziendali, nel contesto della politica "Bring Your Own Device". Devono essere rispettate le seguenti regole:

a) È consentito **da dispositivi privati** l'accesso **esclusivamente** alla posta aziendale ed alle applicazioni rese disponibili su Internet previa autorizzazione del proprio responsabile.

k) È consentita la connessione di PC e dispositivi personali solamente alla rete aziendale Wifi Guest;

l) È consentito l'accesso alla posta aziendale da dispositivi privati, solo tramite autorizzazione scritta della direzione;

m) nel caso in cui si utilizzi il proprio dispositivo personale per l'accesso alla mail e ad altre applicazioni aziendali, qualora questo fosse rubato o smarrito, è necessario:

1. segnalare prontamente lo smarrimento al reparto Sistemi Informativi;
2. modificare prontamente tutte le password memorizzate sul dispositivo.

Riguardo all'utilizzo della password

L'accesso ai dispositivi ed alla rete richiede il possesso di un nome utente (User ID univoco) e di una parola chiave segreta (Password).

Per una corretta e sicura gestione delle proprie password devono essere rispettate le seguenti regole:

a) le password sono personali e **non vanno mai comunicate ad altri**; l'unica eccezione consentita riguarda le password di magazzino, confezionamento e manutenzione;

b) le password devono essere lunghe almeno **8 caratteri** e devono contenere anche lettere maiuscole, caratteri speciali e numeri; verranno descritte regole specifiche in dettaglio;

c) le password non vanno **mai comunicate** a nessuno; qualora vi sia il dubbio che la password non sia più segreta, deve essere immediatamente sostituita;

d) le password devono essere aggiornate al primo utilizzo e successivamente **ogni sei mesi**;

e) Le password non devono essere trascritte su carta o mezzo elettronico (mai, ad esempio, su Post-It o agende (cartacee, posta elettronica, telefono cellulare);

f) vanno evitate password banali, per esempi che riprendano il nome, la userid, o altri dati facilmente ricavabili (data di nascita, nome del coniuge, targa della propria auto, ...):

APS Holding S.p.A.
Società soggetta all'attività di direzione
e coordinamento del Comune di Padova
Società a Socio Unico

Via Salboro 22/b - 35121 Padova | T. +39 049 5660111 - F. +39 049 5660112
E. info@apsholding.it | PEC apsholding@legalmail.it | www.apsholding.it
C.F./P.IVA 03860240286 | REA PD 342892 | Cap. sociale i.v. € 49.508.016

L'azienda può imporre, con opportune modalità tecniche, l'applicazione di tutte o alcune delle regole precedenti. In ogni caso tutte devono essere applicate con diligenza.

Riguardo al supporto tecnico ed alla risoluzione di anomalie

Tutte le comunicazioni con il personale dei Sistemi Informativi devono avvenire tramite la pagina: https://www.apsholding.it/area-riservata-dashboard/richiesta-di-intervento-help-desk/

L'incaricato che rileva attività anomale su un Dispositivo a lui affidato è tenuto ad informare prontamente il personale dei Sistemi informativi.Qualora fossero rilevate attività anomale da parte di un Dispositivo (ad esempio, traffico anomalo, trasmissione di virus o malware, altri eventi che arrechino danno alla normale operatività aziendale o a soggetti terzi), l'azienda si riserva di intervenire e/o di bloccare l'utilizzo dello Strumento Aziendale, al fine di risolvere il problema/disservizio.

Il personale dei Sistemi informativi può collegarsi, visualizzare in remoto ed operare sul Dispositivo affidato all'utente al fine di effettuare l'assistenza tecnica e consentire il ripristino della normale attività. L'intervento può essere effettuato: i) su chiamata dell'Incaricato; ii) in situazione di oggettiva necessità o emergenza; iii) a seguito della rilevazione tecnica di problemi o di allarmi generati dal sistema informatico o dalla Rete Aziendale. In questi ultimi casi verrà data preventiva comunicazione all'Utente della necessità dell'intervento stesso, salvo che ciò non ne pregiudichi la tempestività ed efficacia.

Riguardo all'uso delle cartelle condivise e delle copie di salvataggio

I dati di lavoro dei singoli utenti (sia di interesse personale che di reparto) devono essere, di norma, salvati sulle cartelle condivise di rete (personali o di ufficio). Il dettaglio delle cartelle da usare per le diverse tipologie di files deve essere concordato con il proprio responsabile.

Questo è necessario perché i dati su PC non sono soggetti a copia di sicurezza e quindi i dati in essi contenuti potrebbero andare persi a seguiti di guasti, furti e smarrimenti. Eventuali copie di sicurezza (backup) devono essere quindi svolte manualmente da parte degli utenti.

Invece, i dati presenti sulle cartelle condivise sono soggetti ad un salvataggio periodico automatizzato.

Riguardo all'uso della navigazione su Internet.

In accordo con le "linee guida del Garante per posta elettronica e internet" [Gazzetta Ufficiale n. 58 del 10 marzo 2007], si precisa quanto segue:

a) La connessione ad Internet è un bene aziendale da utilizzare in modo corretto ed appropriato.

b) Non è consentita la navigazione su Internet per scopi privati. È tassativamente vietata l'effettuazione di ogni genere di operazioni finanziaria.

c) Il titolare si riserva di bloccare l'accesso a siti ritenuti inappropriati o non attinenti l'ambito lavorativo. In particolare si **vieta** l'utilizzo dei **social network**, se non espressamente autorizzati, di giochi online e di siti di shopping online.

APS Holding S.p.A.
Società soggetta all'attività di direzione e coordinamento del Comune di Padova
Società a Socio Unico

Via Salboro 22/b - 35121 Padova | T. +39 049 5660111 - F. +39 049 5660112
E. info@apsholding.it | PEC apsholding@legalmail.it | www.apsholding.it
C.F./P.IVA 03860240286 | REA PD 342892 | Cap. sociale i.v. € 49.508.016

È comunque **proibito** l'accesso a reti peer-to-peer di condivisione contenuti, il download di video e musica, il download e l'installazione di software senza esplicita autorizzazione del Responsabile dei Sistemi Informativi. La violazione del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248) costituisce reato.

d)

e) L'azienda si riserva di predisporre controlli a campione sugli accessi ad Internet e sulla navigazione web. L'accesso alla rete e la navigazione vengono registrati in appositi log, che consentono l' analisi, per esempio, dei siti maggiormente visitati, degli orari di utilizzo di Internet, dei download effettuati e delle richieste di siti non consentiti.

Gli archivi che contengono queste ed analoghe informazioni sono gestiti dal personale dei Sistemi informativi. Tali archivi sono protetti da accessi non autorizzati per garantire l'integrità e la riservatezza dei dati. L'accesso ai dati di connessione è limitato agli Amministratori di Sistema, che hanno ricevuto uno specifico incarico per lo svolgimento di tale attività.

Questi dati sono utilizzati esclusivamente, per garantire la sicurezza dei sistemi aziendali, per la ricerca di possibili errori, per analisi di tipo statistico e per verificare eventuali abusi. SI veda al paragrafo sui .

Riguardo all'uso della posta elettronica.

Devono essere rispettate le seguenti regole:

a) I dati scambiati, anche via email, utilizzando gli strumenti aziendali sono di proprietà di APS Holding SpA.

f) **Non è consentito** l'utilizzo della **mail** aziendale a **scopi privati**. È vietato utilizzare l'indirizzo di posta elettronica aziendale per iscriversi a siti o newsletter non attinenti all'attività lavorativa, senza espressa autorizzazione scritta. È proibito l'invio di materiale con contenuto violento o offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o con contenuto politico. Nel caso di ricezione di messaggi con allegati di dubbia provenienza, si raccomanda di consultare gli incaricati dei Sistemi informativi.

g) Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato di APS Holding SpA potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nel presente regolamento.

h) È opportuno rimuovere messaggi non attinenti al rapporto di lavoro. Vanno cancellati messaggi e documenti inutili e ingombranti o non pertinenti.

i) Non è consentito l'invio di **informazioni aziendali** tramite recapiti **di posta privati**.

j) L'accesso alla posta elettronica è consentito, solo in caso per necessità professionali, anche al di fuori della rete della Società, con le medesime credenziali e regole previste all'interno.

APS Holding S.p.A.
Società soggetta all'attività di direzione
e coordinamento del Comune di Padova
Società a Socio Unico

Via Salboro 22/b - 35124 Padova | T. +39 049 5660111 - F. +39 049 5660112
E. info@apsholding.it | PEC apsholding@legalmail.it | www.apsholding.it
C.F./P.IVA 03860240286 | REA PD 342892 | Cap. sociale i.v. € 49.508.016

k) Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per APS Holding SpA. ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile d'ufficio.

l) Il servizio di email può essere soggetto, a discrezione della direzione, a **backup periodico** per motivi di protezione dei dati, insieme ai file accessori di registrazione delle attività (per esempio date e ora, mittente, destinatari, altri interessati, e altri dati analoghi), che restano a disposizione degli amministratori di sistema. Tutti i messaggi di posta elettronica ed i relativi file allegati sono verificati in maniera automatica da programmi anti-codici maligni, quali antivirus, anti-spyware, antispam, antiphishing, distribuiti e gestiti dal reparto Sistemi Informativi. Tali programmi garantiscono la confidenzialità dei contenuti, salvo il caso in cui l'Azienda debba far fronte ad esigenze tecniche o di sicurezza o debba utilizzare dati registrati a fini di esercizio o difesa di un diritto in sede giudiziaria.

m) In caso di assenza prolungata o comunque prevedibile, gli Utenti sono invitati ad attivare la risposta automatica "fuori sede". Nel messaggio di risposta devono essere indicati i riferimenti aziendali di un altro Incaricato a cui è possibile rivolgersi in assenza del destinatario originale.

n) In caso di assenza non programmata, tale attivazione può essere effettuata direttamente dal personale del reparto Sistemi Informativi.

o) Al termine del rapporto di lavoro, i messaggi contenuti nella casella di posta potranno essere resi disponibili ad altro dipendente.

Riguardo alla custodia dei documenti cartacei

I documenti cartacei devono essere conservati negli archivi a questo deputati.

Devono essere rispettate le seguenti regole:

a) dall'archivio vanno prelevati solo i documenti necessari, e per il tempo strettamente necessario. Vanno ricollocati in archivio appena possibile.
b) Va verificata la completezza dei documenti al momento del prelievo e della restituzione in archivio.
c) Nel caso in cui sia necessario lasciare il posto di lavoro (per qualunque motivo) e non sia possibile o conveniente restituire i documenti in archivio, i **documenti devono essere tenuti in luogo sicuro** (per esempio armadio o cassetto o classificatore chiuso a chiave, o in cassaforte).
d) È fatto esplicito **divieto** di lasciare i **documenti sensibili incustoditi** sia durante il giorno che fuori dall'orario lavorativo.
e) È opportuno ridurre al minimo le stampe e le copie cartacee.
f) I documenti cartacei scaduti o non più necessari vanno distrutti in modo tal da non essere più ricostruibili.

Controlli preventivi e difensivi

L'Azienda si riserva di effettuare controlli per verificare l'integrità dei propri sistemi informatici e a fini di ordinaria manutenzione degli stessi. In tale sede si riserva anche di accertare e segnalare

APS Holding S.p.A.
Società soggetta all'attività di direzione
e coordinamento del Comune di Padova
Società a Socio Unico

Via Salboro 22/b - 35128 Padova | T. +39 049 5660111 - F. +39 049 5660112
E. info@apsholding.it | PEC apsholding@legalmail.it | www.apsholding.it
C.F./P.IVA 03860240286 | REA PD 342892 | Cap. sociale i.v. € 49.508.016

eventuali abusi commessi dagli Utenti, garantendo il rispetto dei principi di non eccedenza e pertinenza previsti dal GDPR, nell'effettuare gli eventuali controlli.

Solo nel caso in cui le attività di controllo consentissero di accertare detti abusi o comportamenti illeciti, potranno essere eseguite verifiche più approfondite, onde poter appurare eventuali responsabilità. In tal caso, ai sensi del combinato disposto dei commi 2 e 3 dell'art. 4, L. n. 300/1970, la Società potrà utilizzare i dati così raccolti anche ai fini disciplinari. I dati contenuti nei file di log dei sistemi verranno conservati per un periodo massimo di 6 mesi.

L'Azienda si riserva pertanto di monitorare i propri sistemi e servizi in caso di:

a) necessità di effettuare verifiche sulla funzionalità e sulla sicurezza,
b) constatare l'utilizzo indebito di posta elettronica, Internet, o degli Strumenti Aziendali e/o degli applicativi che ne consentono l'utilizzo,
c) abusi,
d) indizi relativi a fuga di informazioni confidenziali o riservate.

In presenza di sospetti – gravi, precisi e concordanti – relativamente all'esistenza di condotte illecite nell'uso delle apparecchiature, di fuga di informazioni riservate o confidenziali, di violazione degli obblighi di fedeltà posti in essere dall'Utente (c.d. controlli difensivi).

Qualora sussista un sospetto l'Azienda si riserva, inizialmente, di inviare una diffida collettiva dallo svolgere attività non consentite e, successivamente ed esclusivamente in caso di reiterate anomalie e difformità dalle prescrizioni di cui al presente Regolamento, di effettuare controlli più approfonditi che possono consentire l'identificazione dell'Utente che ha violato le prescrizioni. In presenza di tali circostanze, i dati sulle navigazioni saranno trattati, oltre che dal Reparto Sistemi Informativi, eventualmente anche dal Reparto HR e dall'Uffici Legale e dai consulenti Legali esterni per eventuali finalità di difesa in giudizio.

Gestione delle informazioni alla cessazione del rapporto di lavoro.

A seguito della cessazione del rapporto di lavoro presso il titolare, il dipendente deve provvedere a:

a) **eliminare** eventuali messaggi di natura personale inviati, ricevuti o archiviati nella propria casella di posta elettronica in violazione della presente Policy;

b) **eliminare** eventuali contatti personali dalla rubrica del sistema di posta elettronica, dallo smartphone aziendale, memorizzati in violazione della Presente Policy;

c) **restituire** i dati in formato cartaceo, di cui sia venuto in possesso nel corso delle attività;

d) **restituire** gli strumenti aziendali (PC e cellulare) completi con i dati di interesse aziendale;

e) **restituire** una copia dei dati (comprese quelli contenuti nella caselle di posta elettronica) di cui sia venuto in possesso nel corso dell'incarico e **cancellarli** da qualunque supporto di sua proprietà o a lui riservato (a titolo di esempio: chiavette, dischi esterni, computer personale, copie in cloud ecc.).

Nella fattispecie, si precisa che, in questa sede, i dati di cui si tratta possono essere riferiti sia a persone fisiche, identificate o identificabili, sia ad altre informazioni come disegni, documenti,

APS Holding S.p.A.
Società soggetta all'attività di direzione
e coordinamento del Comune di Padova
Società a Socio Unico

Via Salboro 22/b - 35121 Padova | T. +39 049 5660111 - F. +39 049 5660112
E. info@apsholding.it | PEC apsholding@legalmail.it | www.apsholding.it
C.F./P.IVA 03860240286 | REA PD 342892 | Cap. sociale i.v. € 49.508.016

codici di accesso e qualunque altro tipo di informazione di tipo industriale di proprietà di APS Holding SpA, delle sue controllate/correlate e dei suoi clienti/fornitori.

Successivamente alla cessazione del rapporto, le credenziali dell'account di posta elettronica della Persona Autorizzata verranno resettate, impedendo l'accesso da parte dello stesso. Verrà predisposto un messaggio di risposta automatico per 30 giorni, con indicazione che l'ex Incaricato non è più dipendente/collaboratore della Società e fornendo contatto alternativo presso l'azienda. Al termine di tale periodo, il messaggio automatico verrà rimosso.

Come già detto. l'Azienda si riserva di mettere a disposizione di altri dipendenti il contenuto della cassetta postale, al fine di consentire la gestione delle attività aziendali (per esempio commerciali).

Sanzioni

Il mancato rispetto o la violazione delle regole contenute nella presente Policy è perseguibile con provvedimenti disciplinari previsti dal CCNL applicabile a ciascun dipendente per tipologia di lavoro, ed altresì con le azioni civili e penali previste dalle leggi vigenti, qualora si verifichino gli estremi per la sussistenza della responsabilità civile o penale.

Nel caso dei collaboratori esterni/fornitori la violazione delle regole contenute nella presente Policy può comportare sanzioni sul piano contrattuale che possono arrivare fino alla risoluzione del rapporto fatte salve azioni civili e penali previste dalle leggi vigenti, qualora si verifichino gli estremi per la sussistenza della responsabilità civile o penale.

Padova, 23 maggio 2023

Protocollo n. 3873

L'Amministratore Delegato
Dottor Riccardo Bentsik

Dichiarazione di presa visione

(Ai sensi del Regolamento Europeo 679/2016)

☑ L'interessato dichiara di aver letto e compreso l'informativa e prende atto delle istruzioni sopra riportate.

Firma per presa visione

_____

APS Holding S.p.A.
Società soggetta all'attività di direzione
e coordinamento del Comune di Padova
Società a Socio Unico

Via Salboro 22/b - 35121 Padova | T. +39 049 5660111 - F. +39 049 5660112
E. info@apsholding.it | PEC apsholding@legalmail.it | www.apsholding.it
C.F./P.IVA 03860240286 | REA PD 342892 | Cap. sociale i.v. € 49.508.016