POLICY AZIENDALE HARDWARE E SISTEMI IT

INDICE

Il presente regolamento è volto a disciplinare l'utilizzo della strumentazione informatica aziendale, da parte dei dipendenti e dei fruitori della stessa in occasione di rapporti di lavoro anche non dipendente. I destinatari del presente regolamento sono d'ora innanzi indicati come UTENTI.

1. UTILIZZO STRUMENTAZIONE HARDWARE (ANCHE PC PORTATILI)

- È fatto divieto installare sulla strumentazione in uso, hardware fisso o removibile (ad esempio apparecchi Wi- Fi) qualora ciò non risulti espressamente richiesto ed autorizzato dall'Azienda.
- L'Azienda si riserva di eliminare qualsiasi elemento hardware la cui installazione non sia stata appositamente prevista o autorizzata.
- In caso di allontanamento dalla propria postazione hardware, è fatto obbligo all'Utente di attivare il salva- schermo (Screen-saver) protetto da password e blocco del PC. In particolare, ogni volta che c'è l'esigenza di allontanarsi dalla stanza, anche per poco tempo, l'Utente deve chiudere la sessione di lavoro e applicare gli accorgimenti per rendere il pc protetto da accessi abusivi, come ad esempio chiudere a chiave la porta della stanza in caso di allontanamento.
- Sui PC dotati di scheda audio e/o di lettore CD non è consentito l'ascolto di programmi, files audio o musicali, se non a fini esclusivamente lavorativi.
- Qualora si rendessero necessarie modifiche alle configurazioni impostate sul PC in uso, occorre darne comunicazione al Titolare del Trattamento e/o all'Amministratore di Sistema.
- Il PC deve essere spento ogni sera prima di lasciare gli uffici (salvo diverse disposizioni o in caso di particolari necessità previamente comunicate dall'Azienda). Prima di effettuare la pausa pranzo è opportuno procedere al salvataggio e alla chiusura di tutti i files aperti, per non ostacolare eventuali attività di amministrazione. Quindi si deve bloccare il PC, in modo da rendere necessario inserire identificatore e credenziale di autenticazione dell'Utente per renderlo di nuovo operativo. Per bloccare il PC l'Utente deve effettuare le seguenti operazioni:

- digitare "CTRL+ALT+CANC"
- scegliere "Blocca computer"

- Per il ripristino delle funzionali, l'Utente dovrà solo immettere le proprie credenziali nell'apposita maschera.
- Gli assegnatari di PC portatili devono conservare e proteggere i Pc a loro consegnati in modo tale da ridurre al minimo rischi di perdita, danneggiamento e/o furto del PC stesso.

2. ACCESSO ED USO DEI SISTEMI INFORMATICI AZIENDALI (CREDENZIALI DI AUTENTICAZIONE)

- I requisiti minimi di complessità delle password sulla base della vigente normativa privacy sono:
  - redazione con caratteri maiuscoli e/o minuscoli;
  - composizione con inclusione di simboli, numeri, punteggiatura e lettere;
  - caratteri non inferiori ad 8 (ad eccezione dei sistemi operativi che non supportano tali requisiti);
  - password non agevolmente riconducibile all'identità del soggetto che la gestisce.
- Pertanto, la password non deve essere basata su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente il soggetto titolare della password stessa. A mero titolo esemplificativo e non esaustivo la password non deve essere: il nome o il cognome dell'Utente, il soprannome la data di nascita propria, dei figli o degli amici consistere in un nome di un hobby o di una passione conosciuta o facilmente conoscibile dai colleghi consistere nel nome e cognome di personaggi famosi.
- Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a cambiarla.
- Non debbono essere utilizzate nella configurazione delle caselle di posta elettronica le opzioni di "compilazione automatica" o remember password, presenti nei browser o in altre applicazioni che gestiscono la procedura di autenticazione.
- L'Utente ha l'obbligo di non alterare la funzione "cambio password" che obbliga a modificare la password periodicamente.
- Ogni Utente può modificare la propria password in qualunque momento. In alcuni casi sussiste l'obbligo di avvisare Titolare del Trattamento e l'Amministratore di Sistema:
  - quando la credenziale per ragioni di servizio è stata trasmessa ad un collega in caso di personale assenza;
  - quando la credenziale per ragioni di servizio è stata forzata, su richiesta del Titolare del trattamento o dall'Amministratore di Sistema;
  - in caso che incaricati o addetti non autorizzati ne siano venuti a conoscenza.
- Un messaggio automatico indica che il tempo di utilizzo della Password sta per spirare: in tale lasso di tempo l'Utente è obbligato a modificare la propria password di accesso.
- L'Amministratore di Sistema può in qualunque momento sulla base di esigenze aziendali, resettare tutte le password di accesso al sistema e alle sessioni di lavoro. In tal caso sarà richiesto all'Utente di scegliere e adottare una nuova password di acceso.
- In caso di mancato utilizzo delle credenziali di autenticazione per il tempo di sei mesi, queste verranno disattivate dall'Amministratore di Sistema. La stessa procedura si attiva nel caso in cui vi sia la perdita della qualità di Utente.

3. INSTALLAZIONE PROGRAMMI

- Sul pc in uso non devono essere installati programmi che non siano ufficialmente forniti dal Titolare del trattamento.

- È vietato il download e l'utilizzo di programmi, ancorché gratuiti, se non per esigenze esclusivamente aziendali e previa esplicita autorizzazione del Titolare del Trattamento.
- L'Azienda, peraltro, ricorda all'utilizzatore che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/1941 come novellata.
- Eventuali illeciti, che dovessero essere commessi per il tramite della strumentazione informatica aziendale, saranno prontamente denunciati alla Polizia Postale competente.

4. APPLICAZIONI

Nel caso in cui l'utente fosse stato dotato dall'azienda di un dispositivo smartphone o tablet:

- Si ricorda di seguire le regole di buona condotta anche nel caso in cui l'utente decida di installare ulteriori App. facendo attenzione che molte applicazioni sono in grado di rilevare automaticamente la posizione geografica e di trasmettere a soggetti terzi i dati raccolti.
- Si raccomanda di utilizzare consapevolmente i dispositivi assegnati per preservare la riservatezza dei dati aziendali ma anche per tutelare i propri dati personali ed evitare comportamenti illeciti come la condivisione di contatti, foto, video e documenti di vario genere senza il consenso di tutte le persone coinvolte.
- Si veda a tale proposito l'**allegato 1** che riporta alcune semplici regole da ricordare.

5. UTILIZZO SUPPORTI MAGNETICI E DATI

- È fatto obbligo conservare, custodire e controllare i supporti informatici removibili contenenti dati, informazioni, notizie o immagini di attinenza aziendale, affinché nessun soggetto terzo ne prenda visione o possesso.
- Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc in uso all'Utente.
- Tutti i files di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte del Titolare del Trattamento e/o all'Amministratore di Sistema.

6. UTILIZZO RETE INTERNA

- La rete interna, istituita appositamente per permettere collegamenti funzionali tra utenti che prestano servizio all'interno della struttura lavorativa, non può esser utilizzata per scopi diversi da quelli ai quali è destinata.
- Qualora nella rete interna debbano circolare dati, notizie ed informazioni aziendali, deve essere premura di ciascun Utente preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

7. UTILIZZO RETE ESTERNA INTERNET

- È fatto divieto memorizzare dalla rete documenti, file o dati comunque non attinenti lo svolgimento delle attività aziendali, in particolare:
    - non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
    - non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo nei casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto;
- l'utilizzo della rete Internet deve essere limitato al tempo strettamente necessario alle operazioni professionali da svolgere.
- Si rende nota l'attivazione di filtri idonei ad evitare navigazioni in siti non correlati all'attività lavorativa e che parimenti sono state create black-list di siti l'accesso ai quali è negato dal sistema.

Rev	Data	Descrizione	Redatto	Verificato	Approvato
0	16/12/2022	Prima emissione	A. Pillan	M. Battiston	D. Anese

- Parimenti si rende nota che sono attivabili sistemi di verifica diretta dei log di connessione effettuati da una singola postazione. Tali verifiche saranno attuate qualora risultino anomalie in relazione alle navigazioni, con particolare riferimento a navigazioni su siti illeciti o non attinenti in alcun modo all'attività svolta dalla singola postazione.
- Eventuali attivazioni di controlli specifici saranno preventivamente notificate.
- I log di connessione di cui sopra, saranno conservati nel rispetto dei limiti previsti dalla normativa vigente.

8. UTILIZZO POSTA ELETTRONICA

- Le caselle di posta elettronica date in uso all'Utente sono destinate ad un utilizzo di tipo aziendale. Non sono tollerati invio e ricezione di e-mail personali. Alle eventuali mail personali ricevute non è assicurata la riservatezza in quanto la ricezione avviene "in chiaro".
- Si rappresenta, inoltre, che:
  - non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita;
  - non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum, newsletter o mail-list, non attinenti all'attività lavorativa.
- In caso di assenza, all'Utente sono poste a disposizione apposite funzioni di sistema che consentano di inviare automaticamente messaggi di risposta.
- La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, è preferibile non usarla per inviare documenti di lavoro "Strettamente Riservati".
- I messaggi di posta elettronica in uscita saranno memorizzati sul server aziendale a cura dei servizi informativi. Ciò al fine di consentire la conservazione ed il back-up dei contenuti il cui recupero e la cui integrità sono essenziali per l'attività aziendale.
- Per quanto riguarda i messaggi di posta elettronica in entrata, la memorizzazione dovrà avvenire sul pc in locale, con conservazione per un minimo di 24 mesi decorrenti dalla ricezione.
- Per la posta elettronica esterna le credenziali di autenticazione sono stabilite dal Titolare del Trattamento. Nel caso in cui sia l'Utente a scegliere la password, lo stesso è obbligato a trasmetterlo a l Titolare del Trattamento stesso, oppure all'Amministratore di Sistema.
- È possibile utilizzare la ricevuta di ritorno per avere la conferma della avvenuta lettura del messaggio da parte del destinatario.
- La casella di posta di pertinenza del proprio ambito deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti.

9. MINACCE ED ATTACCHI VIRALI

- Il sistema informatico-telematico aziendale è protetto da attacchi di virus informatici e da attacchi dall'esterno attraverso apparecchiature Firewall, questo per garantire l'incolumità e protezione dei dati in esso contenuti nel rispetto del patrimonio aziendale e della legge sulla Privacy.
- Al fine di garantire lo standard di protezione adottato non è possibile effettuare operazioni non controllabili che possano mettere in pericolo l'incolumità del sistema, salvo autorizzazione del Titolare del Trattamento. In particolare, è necessario seguire le seguenti regole:
  - non scaricare files dalla rete internet di qualsiasi natura;
  - non comunicare attraverso chat-line o altri sistemi simili se non con sistemi garantiti e certificati;
  - non accedere a siti che richiedono l'installazione di certificati, quali ad esempio: remote banking, internet banking, transazioni finanziarie, acquisti online di qualsiasi natura e genere;

- non iscriversi a siti internet, newsletter, bacheche elettroniche, guest book, community e ad altra attività similare che richiede il rilascio di identificazione personale o aziendale;
- non introdurre qualsiasi supporto digitale di tipo personale, fosse anche in sola lettura, quali ad esempio: CD-ROM, chiavette USB, HD esterni, cellulare, macchine fotografiche digitali.

- In caso di rilevamento di virus su un qualsiasi PC, il software di protezione installato, lo segnala in maniera evidente, e l'utente è tenuto ad avvisare il Titolare del Trattamento, il quale provvederà, a seconda dei casi, ad agire di conseguenza; in questo caso, oltre che rimuovere immediatamente il Virus (sempre mediante il programma Anti-Virus), verrà avviata una ricerca per scoprirne la provenienza, al fine di evitare il ripetersi dell'incidente.
- Qualora sorgesse la necessità di installare un nuovo software o di modificare la configurazione di un Personal Computer, deve essere richiesta ed ottenuta l'autorizzazione da parte del Titolare del trattamento o del Responsabile Privacy ove presente.
- Ogni Utente di PC deve cancellare qualsiasi software che abbia modificato la configurazione originale, che sia stato installato in un secondo tempo senza la consultazione della Direzione o che sia scaricato da Internet ed installato.

10. WEBCAM

- Per l'uso delle Webcam o di altri sistemi di audio-videoripresa installati o collegati come hardware agli elaboratori aziendali, si richiama alla massima attenzione; si ricorda che queste apparecchiature possono ricadere sotto al provvedimento del Garante della videosorveglianza del 08 aprile 2010.
- Di conseguenza si richiede ad ogni Utente dotato di tali sistemi di:
  - utilizzare le webcam solo per necessità collegate strettamente alle attività lavorative;
  - di non lasciare collegato il sistema di audio-videoripresa se non necessario;
  - di ricordarsi dopo l'uso dello stesso di chiudere la connessione aperta.

11. APPLICAZIONE ED INTERPRETAZIONE DEL PRESENTE REGOLAMENTO

- Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, l'Utente può rivolgersi al Titolare del Trattamento e/o all'Amministratore di Sistema.
- Qualora l'Utente violi anche una sola delle presenti prescrizioni, potranno essere emanati richiami disciplinari in conseguenza del mancato rispetto di quanto ivi contenuto.
- Resta inteso che qualora la violazione integri anche un reato, l'Azienda si riserva di procedere per la salvaguardia della propria posizione e di terze parti offese (in tal senso si fa particolare riferimento al download di opere protette – musica o film – nonché di navigazioni su siti illeciti).

12. DISCIPLINA DEROGHE E MODIFICHE DEL PRESENTE DOCUIMENTO

- Qualora al presente regolamento l'Azienda intenda apporre modifiche, queste saranno applicate dandone conoscenza immediata all'Utente.
- Deroghe o modifiche di uno o più punti del presente regolamento, non rendono invalidi gli altri punti.

Concordia Sagittaria, 16/12/2022 La Direzione _____

Rev	Data	Descrizione	Redatto	Verificato	Approvato
0	16/12/2022	Prima emissione	A. Pillan	M. Battiston	D. Anese

ALLEGATO 1: I SUGGERIMENTI DEL GARANTE PER TUTELARE LA TUA PRIVACY QUANDO USI APP PER SMARTPHONE E TABLET

Ogni giorno su smartphone e tablet utilizziamo tantissime applicazioni (definite anche App). Sono strumenti utili, divertenti, a volte indispensabili. Esiste una App praticamente per tutto: per informarsi, giocare, rimanere in contatto con le altre persone, prenotare ristoranti e alberghi, comprare beni e servizi, effettuare operazioni bancarie, dare sfogo alla creatività…

Ma spesso quando utilizziamo una App forse non ci preoccupiamo anche di tutelare la nostra privacy…

Per esempio: fai attenzione a quanti e quali dati una App potrà trattare?
Una App può richiedere accesso alle immagini e ai file che conservi in memoria, ai contatti in rubrica, ai dati sulla geolocalizzazione, al microfono e alla fotocamera del tuo smartphone o del tuo tablet. Prima di installarla, cerca di capire quanti e quali dati verranno raccolti e come verranno utilizzati.
Se una App richiede dati non necessari rispetto ai servizi offerti, evita di installarla. Alcune informazioni raccolte dalle App potrebbero anche finire automaticamente online se le impostazioni lo prevedono. Potresti così rivelare a tutti informazioni personali anche senza accorgertene.

Alcuni spunti di riflessione
Sai che se la App del tuo social network è connessa con il sistema di geolocalizzazione dello smartphone o del tablet potresti far sapere involontariamente a tutti dove ti trovi?
Hai mai pensato che i dati raccolti dalle App che misurano le tue prestazioni sportive o monitorano il tuo stato di salute potrebbero essere trasmessi a terzi per finalità che non sempre conosci?
Se usi una App per la condivisione di foto e video, ti chiedi sempre prima se le persone riprese sono d'accordo a diffondere la propria immagine online?

Prima di installare e utilizzare una App, leggi sempre le condizioni d'uso e verifichi se è presente una privacy policy? Informati su chi tratterà i tuoi dati personali e con quali finalità. Cerca anche di capire per quanto tempo verranno conservati i dati personali che ti riguardano e se possono essere condivisi con terze parti per finalità commerciali o di altro tipo.

Sai che insieme alle App potresti scaricare virus e malware pericolosi per la tua privacy?
Per evitare rischi, è bene fare attenzione alla fonte di provenienza delle App e installare software anti-virus in grado di proteggere i dati personali da eventuali violazioni.

Ti domandi da dove provengono le tue App?
Se non sei sicuro dell'affidabilità della fonte, è meglio rivolgersi ai market che offrono maggiori garanzie di controllo sul software e consentono di leggere i giudizi degli altri utenti, utili per valutare la qualità delle App, ma anche eventuali rischi per la privacy. Se il market prevede la creazione di un account, informati sempre su come tratterà i tuoi dati.

Ti preoccupi di evitare che i minori possano scaricare e utilizzare le App da soli?
I più piccoli, infatti, sono meno consapevoli e più esposti al rischio di una raccolta e diffusione incontrollata di dati personali.

Il primo strumento per tutelare la privacy è la consapevolezza.
Cerchiamo quindi di informarci e ricordiamoci sempre che "c'è una App per tutto… ma attenzione ai dati personali!!

Rev	Data	Descrizione	Redatto	Verificato	Approvato
0	16/12/2022	Prima emissione	A. Pillan	M. Battiston	D. Anese