

REGOLAMENTO SULL'UTILIZZO DI POSTA, INTERNET, STRUMENTI E DISPOSITIVI INFORMATICI DA PARTE DEI DIPENDENTI, ISTRUZIONI PER LA SICUREZZA INFORMATICA**Sommario**

Scopo	2
Campo di applicazione	2
Generalità	2
Gestione delle password personali	3
Struttura delle password	3
Password degli utenti	3
Personal Computer (PC) o Desktop Virtuale	3
Connessione al Desktop Virtuale	4
Disconnessione dal Desktop Virtuale	4
Spazi di Archiviazione e Supporti di Memorizzazione Esterni	4
Servizi Gratuiti di Trasferimento di File di Grandi Dimensioni	4
Connessione internet	4
Dalla rete di Persico verso l'esterno	4
Dall'esterno verso la rete di Persico	5
Posta elettronica	5
Stampe cartacee	6
Gestione dei file e scambio dati	6
Conservazione dei file	6
Scambio dei dati tra interni	6
Gestione della propria postazione di lavoro	6
Scrivania, cassetiera ed eventuale armadio	7
Gestione della quotidianità	7
Cellulare aziendale	7
Cestino dei rifiuti. Documenti da eliminare e carta da riciclare	7
Fotografie e filmati	7
Cambio di mansione/attività/incarico di lavoro	8
Smart Working	8
Violazioni e sanzioni disciplinari	8

Scopo

La presente istruzione regola le responsabilità, doveri e comportamenti del personale dipendente/collaboratore di Persico in materia di utilizzo di posta, internet, strumenti e dispositivi informatici (ivi compresi eventuali telefoni cellulari di servizio), anche ai fini della sicurezza informatica dell'organizzazione, nonché dei possibili controlli effettuabili da parte dell'amministrazione.

Il tutto nel rispetto delle seguenti normative:

1. la Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento"; in particolare l'art. 4, comma 1, della Legge 300/1970, secondo cui la regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali;
2. il Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR); in particolare viene garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 2016/679;
3. le "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007 ed i Provvedimenti ivi connessi;
4. l'articolo 23 del D.lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa»;
5. l'articolo 32 GDPR che prescrive che il Titolare del trattamento deve adottare misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, la conformità del trattamento al Regolamento, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le dette misure debbono essere periodicamente riesaminate e aggiornate.

Campo di applicazione

Il presente documento è da ritenersi applicabile a tutti i dipendenti/collaboratori di Persico.

Inoltre, stabilisce la possibilità di applicare provvedimenti disciplinari qualora vengano violate le norme qui previste.

Generalità

I dispositivi hardware e software ed in generale tutti gli strumenti di lavoro disponibili presso Persico sono utilizzabili esclusivamente per le attività finalizzate al compimento degli incarichi di lavoro assegnati; altri utilizzi sono da considerarsi esclusi.

In caso di esigenze particolari, è consentito l'uso di pc personali, ma ciò soltanto previa autorizzazione dell'Ufficio IT e previa adeguata configurazione degli stessi da parte del personale tecnico informatico incaricato.

Durante il lavoro è inoltre vietato:

- Utilizzare dati personali degli utenti, degli amministratori e dei dipendenti in modo diverso/difforme da quanto necessario per l'espletamento del proprio lavoro e/o da scopi non autorizzati;
- Trattare impropriamente i dati personali degli utenti, degli amministratori e dei dipendenti;
- Diffondere e/o portare all'esterno di Persico i dati personali degli utenti, degli amministratori e dei dipendenti, salvo quando necessario per l'espletamento del proprio lavoro;

- Modificare i dati personali degli utenti, degli amministratori e dei dipendenti senza la necessaria autorizzazione.

Va ricordato che la politica generale di Persico sull'accesso ai dati è quella basata sul principio di pertinenzialità e non eccedenza, ovvero è consentito l'accesso a quel dato, quel documento, quel PC, ecc. se e solo è indispensabile per lo svolgimento delle attività assegnate.

Pertanto, se si viene in possesso di un bene e/o un'informazione non necessaria (sia da una persona interna a Persico, sia da un soggetto esterno, è tassativo:

- Informare subito il mittente che non si è autorizzati a tenere/accedere a tale bene/informazione;
- Invitare il mittente a non consegnare/inviare più quel tipo bene/informazione;
- Riconsegnare/eliminare prontamente il bene/informazione.

Tutti i dipendenti e gli amministratori sono tenuti a rispettare le istruzioni che seguono, comprese quelle in materia di sicurezza informatica.

Gestione delle password personali

Le password sono personali, non devono essere comunicate a nessuno e non devono in alcun modo essere conoscibili da parte di terzi.

Le credenziali di accesso devono essere mantenute segrete e custodite adeguatamente, in modo che non vengano utilizzate per accedere al pc assegnato al dipendente o al collaboratore.

La password di accesso ai pc deve essere **OBBLIGATORIAMENTE** modificata ogni TRE mesi.

Va ricordato che, qualora non si acceda da 6 mesi ad un'area protetta, la password deve essere resettata dall'Amministratore di Sistema.

Qualora ci sia anche il minimo dubbio che la propria password possa essere conosciuta da altri, questa deve essere immediatamente modificata.

Anche i telefoni cellulari di servizio devono essere **OBBLIGATORIAMENTE** protetti da apposito codice di accesso compatibile con la tecnologia del telefono.

Struttura delle password

La password deve essere sempre composta da almeno 8 caratteri alfanumerici. La password deve contenere:

Almeno un numero da 0 a 9

Almeno un carattere alfabetico minuscolo e almeno un carattere alfabetico MAIUSCOLO

Almeno un carattere speciale

Esempio: Ay3rdefw.

La password non deve contenere riferimenti riconducibili alla propria persona o all'organizzazione di appartenenza o alla funzione o mansione svolta.

La password non deve essere costruita applicando criteri e/o logiche che possono essere utilizzate per individuare la password in vigore (es: password vecchia: MLpass01 - password nuova: MLpass02)

Le password utilizzate devono essere diverse da quelle utilizzate per scopi personali al di fuori dell'ambito aziendale (social, blog, banca, ecc.)

Password degli utenti

È vietato chiedere o raccogliere in qualsiasi modo le password degli utenti.

Se è necessario accedere alle procedure dell'utenza, l'utente deve essere invitato a digitare lui stesso la password.

Personal Computer (PC) o Desktop Virtuale

Il PC è personale ed ogni dipendente/collaboratore ne è responsabile.

Connessione al Desktop Virtuale

Per garantire la sicurezza informatica, salvo casi di emergenza la connessione al desktop virtuale per il personale che opera in smart working deve essere effettuata attraverso appositi canali VPN.

Disconnessione dal Desktop Virtuale

Si ricorda che al termine dell'utilizzo del proprio desktop virtuale, è necessario effettuare la disconnessione dai sistemi e programmi di Persico.

Spazi di Archiviazione e Supporti di Memorizzazione Esterni

Per lo scambio di file e documenti devono essere creati appositi spazi di archiviazione condivisa sul server al fine di limitare il più possibile l'utilizzo di chiavette USB o altri dispositivi rimovibili.

L'uso di chiavette USB o altri dispositivi rimovibili è fortemente sconsigliato in quanto potenzialmente molto pericoloso per la sicurezza dei sistemi informatici e della rete di Persico.

Qualora Persico ritenga necessario l'utilizzo di tali dispositivi, detti dispositivi dovranno essere forniti e custoditi dal personale di Persico a ciò espressamente incaricato.

Tali dispositivi possono essere utilizzati soltanto per motivi attinenti alle esigenze di Persico e, nel caso in cui vengano utilizzati anche al di fuori di Persico, devono essere controllati dal sistema antivirus sia al termine delle operazioni che all'inizio del loro utilizzo, prima di aprirne il contenuto.

In generale devono essere utilizzati il meno possibile, vista la possibile facilità di perdita del supporto o di infezione; a tali soluzioni per lo scambio di dati va preferita la posta elettronica o l'SFTP.

Prima della consegna dei file al destinatario, è compito di ogni dipendente/collaboratore verificare ed accertarsi che siano presenti sui supporti di memorizzazione esterni (utilizzati per lo scambio) **solo ed esclusivamente i file da consegnare e nessun altro file.**

I supporti devono essere conservati con cura e non lasciati nella disponibilità di altre persone, anche per brevi periodi, soprattutto quando si è all'esterno di Persico (riporli sempre nella borsa lavoro, borsa notebook, ecc.).

Eventuali CD-ROM e DVD da eliminare vanno distrutti nel distruggi-documenti o rotti in più pezzi.

Eventuali key-memory o hard disk esterni non funzionanti vanno immediatamente consegnati all'Amministratore del Sistema.

Servizi Gratuiti di Trasferimento di File di Grandi Dimensioni

È assolutamente vietato scambiare file contenenti dati personali di qualsiasi natura attraverso servizi gratuiti di trasferimento di file di grandi dimensioni, salvo previa autorizzazione di un amministratore di sistema.

Connessione internet

Dalla rete di Persico verso l'esterno

La navigazione in Internet è uno strumento necessario allo svolgimento della propria attività lavorativa. È proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. È fatto divieto all'utente lo scarico di software (anche freeware o shareware) prelevato da siti Internet, se non espressamente autorizzato dall'Ufficio IT.

È vietato eseguire download/upload di file eseguibili o file/documenti da siti Web o Ftp, salvo siano strettamente inerenti le attività di Persico (leggi, circolari di enti pubblici, documentazione ministeriale, documentazione tecnica, etc.).

È vietata l'effettuazione di ogni genere a titolo personale di transazioni finanziarie ivi comprese le operazioni di remote banking, acquisti on-line o simili, salvo casi espressamente autorizzati.

È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietato la partecipazione a forum non professionali, l'utilizzo di chat line, giochi, social forum e registrazioni in guest books, anche utilizzando pseudonimi (o nicknames).

È vietato il download, la trasmissione e la conservazione di file musicali o file multimediali, anche attraverso strumenti peer-to-peer (emule, torrent, ecc.).

Durante la navigazione web, è vietato selezionare flag e/o “pulsanti opzione” che memorizzano user e/o password (es: “ricordati me”, “ricorda user/password”, ecc.), ad eccezione dell'utilizzo di sistemi di password manager fornito da provider che offrano un sistema di doppia autenticazione.

Dall'esterno verso la rete di Persico

Qualora sia necessario accedere alla rete di Persico attraverso internet, è necessario prestare la massima attenzione nelle fasi di accesso, proteggendo da occhi o da telecamere presenti la fase di digitazione della login e della password.

Una volta aperta la connessione, questa deve rimanere attiva lo stretto necessario all'espletamento delle attività richieste, quindi chiusa.

In ogni caso, prima di abbandonare la postazione dalla quale è stata aperta la connessione è bene accertarsi dell'avvenuta chiusura della stessa, eliminando la cronologia e i file temporanei (ove possibile).

Webcam

Le eventuali webcam messe a disposizione per lo svolgimento delle attività di lavoro devono essere utilizzate solo ed esclusivamente per tali fini e sono da ritenersi esclusi altri impieghi.

Durante una connessione con uso di webcam, è compito del dipendente/collaboratore verificare cosa viene inquadrato dalla webcam ed eventualmente correggere la posizione della stessa qualora inquadrino altre persone o documenti contenenti dati personali.

Posta elettronica

La casella di posta assegnata al dipendente/collaboratore è uno strumento di lavoro ed ogni dipendente/collaboratore ne è responsabile. Le persone assegnatarie della casella di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare la casella di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione. È buona norma evitare messaggi completamente estranei al rapporto di lavoro od alle relazioni tra colleghi.

In caso di ricezione di email non attinenti alle attività di lavoro (spam), queste vanno immediatamente segnalate agli amministratori di sistema; **non si devono in alcun modo attivare gli allegati di tali messaggi.**

Se l'email ricevuta è destinata ad altre persone è necessario limitare il più possibile la lettura del documento, ovvero facendolo con il solo obiettivo di comprendere che non si tratta di documentazione propria (quindi senza né leggere il contenuto, né cercare di capire a chi appartiene), ma inviare un messaggio al mittente spiegando l'errore. L'email ricevuta va immediatamente eliminata, anche dal cestino.

In previsione della cessazione del rapporto di lavoro e nel caso in cui per esigenze organizzative sia necessario trasferire il contenuto della casella di posta personale (nome e cognome), di concerto con il diretto superiore il dipendente dovrà eliminare dalla casella di posta elettronica personalizzata tutti i messaggi personali o non rilevanti ai fini di Persico e a consegnare al diretto superiore il contenuto residuo della casella di posta, che verrà messo a disposizione del personale subentrante.

L'account di posta del dipendente verrà disattivato contestualmente alla cessazione del rapporto di lavoro e la sua casella di posta continuerà ad essere attiva per i tre mesi successivi al solo fine di recapitare ai mittenti dei messaggi l'avviso di mancato recapito del messaggio per cessazione del rapporto e la fornitura delle coordinate alternative da contattare, senza che l'organizzazione possa visualizzare il contenuto dei messaggi in arrivo.

Delle operazioni di cui sopra verrà redatto apposito verbale ed una copia del verbale stesso verrà consegnata al dipendente in uscita.

In caso di assenza pianificata o per breve malattia il dipendente è tenuto ad attivare la funzionalità di sistema del proprio account di posta che consente di avvisare automaticamente il mittente della Sua

assenza e che consente l'eventuale comunicazione delle coordinate di Persico alternative da contattare durante la Sua assenza.

Qualora il dipendente fosse impossibilitato a compiere le attività di cui sopra e la sua assenza dovesse prolungarsi oltre il termine di tre giorni lavorativi, il dipendente nominerà, in piena libertà di forme, un proprio fiduciario che verificherà il contenuto dei messaggi presenti nella casella di posta ed inoltrerà all'organizzazione quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tali attività verrà comunque redatto apposito verbale ed il dipendente verrà informato del numero e della natura dei messaggi inoltrati alla prima occasione utile.

Qualora il dipendente fosse impossibilitato a compiere tutte le attività di cui sopra e la Sua assenza perdurasse oltre un certo termine (da stabilirsi), l'organizzazione potrà, in caso di necessità e per motivi di sicurezza ed organizzativi, disporre l'attivazione dei sistemi automatici accedendo all'account del dipendente per il tramite dell'amministratore di sistema oppure nominare un fiduciario previo accordo con il DPO. Di tali attività verrà comunque redatto apposito verbale ed il dipendente verrà informato di quanto accaduto alla prima occasione utile.

Si ricorda che tutto il server di posta è sottoposto a backup.

Si ricorda che sul server di posta viene mantenuta traccia delle e-mail inviate su un database di log. Periodici Controlli di detti log possono essere effettuati allo scopo di verificare la sicurezza e la correttezza dell'uso delle email; altri controlli possono essere effettuati, su richiesta, dall'Autorità Giudiziaria.

Stampe cartacee

Quando viene lanciata una stampa ad una stampante, è buona norma provvedere il prima possibile al ritiro della documentazione stampata.

Al momento del ritiro della documentazione bisogna che non siano presenti stampe di altre persone tra i propri documenti; qualora si verificasse tale eventualità, limitare il più possibile la lettura dei documenti, con il solo obiettivo di comprendere che non si tratta di documentazione propria (quindi senza leggere il contenuto, né cercare di capire a chi appartengono), lasciandoli nella stampante.

Gestione dei file e scambio dati

Conservazione dei file

In generale i file relativi alle attività di lavoro della giornata non devono essere lasciati sul proprio Personal Computer, ma salvati nella cartella nella specifica area dedicata nelle cartelle sul server, nella specifica area dedicata.

Si ricorda che il PC non è soggetto a back-up e quindi non è garantita la conservazione dei file eventualmente lasciati sull'hard disk. Inoltre, non è consentito avere cartelle condivise sul proprio PC.

Scambio dei dati tra interni

L'utilizzo delle cartelle di scambio tra colleghi di gruppi diversi deve avvenire attraverso cartelle pubbliche su server. L'operazione di recupero / prelievo deve essere eseguita mediante un "taglia-incolla" e non con un "copia-incolla". Il trasferimento del file deve avvenire in modo da ridurre al minimo la durata della permanenza del file da scambiare nella zona comune.

Gestione della propria postazione di lavoro

La postazione di lavoro include i seguenti elementi:

Scrivania

Cassettiera

Eventuale armadio personale

Eventuale cellulare di Persico

Cestino dei rifiuti

Scrivania, cassetiera ed eventuale armadio

La scrivania, la cassetiera (e l'eventuale armadio dedicato) è personale ed ogni dipendente/collaboratore ne è responsabile.

Al primo accesso alla propria postazione deve essere verificato:

Che non siano presenti documenti appartenenti al precedente utilizzatore. In caso si rilevi tale situazione deve essere immediatamente contattato il Responsabile di Area.

Che le serrature della cassetiera e dell'eventuale armadio siano funzionanti e le chiavi siano tutte presenti (una chiave per tipo).

Gestione della quotidianità

La documentazione di lavoro presente sulla scrivania deve essere in ordine, evitando di lasciare oggetti personali assieme al materiale di lavoro (cellulari personali, apparecchiature personali, Supporti di memoria personali, apparecchiature radio).

I dati personali degli utenti, dei collaboratori, degli amministratori e dei dipendenti, se non utilizzati, non devono essere lasciati incustoditi sulla scrivania, ma devono essere protetti (nella cassetiera o nell'armadio).

Durante l'orario di lavoro, i dati personali degli utenti, degli amministratori, dei collaboratori e dei dipendenti utilizzate non vanno lasciati incustoditi durante le eventuali pause/assenze dal posto di lavoro (coperti, riposti in cassetiera o nell'armadio).

È vietato leggere/fotocopiare/prendere possesso di documenti/appunti presenti nella postazione di altri, salvo espressa autorizzazione di chi ha in gestione tali documenti.

Prima di lasciare la postazione di lavoro per un periodo prolungato (uscite per il pranzo, riunioni lunghe, etc.) e comunque sempre al termine della giornata di lavoro, è necessario riporre i dati personali degli utenti, degli amministratori, dei collaboratori e dei dipendenti presenti sulla scrivania nella cassetiera o nell'armadio; quest'ultimi vanno chiusi e le chiavi conservate con cura.

Cellulare aziendale

Il cellulare in dotazione è personale ed ogni dipendente/collaboratore ne è responsabile.

Il dipendente/collaboratore dotato di cellulare dall'organizzazione è tenuto a rispondere a tutte le chiamate e, qualora impossibilitato a rispondere, a ricontattare il prima possibile i numeri chiamanti.

Il cellulare deve essere utilizzato soltanto per ragioni di lavoro, deve essere conservato con cura e deve avere attiva la protezione della SIM mediante digitazione del PIN.

In caso di sostituzione, la memoria del telefono deve essere completamente cancellata e l'apparecchiatura consegnata agli amministratori di sistema.

L'organizzazione si riserva di effettuare controlli occasionali sul corretto uso del cellulare consegnato al dipendente/collaboratore.

Cestino dei rifiuti. Documenti da eliminare e carta da riciclare

Prima di eliminare un documento cartaceo va prima attentamente valutato il contenuto del documento.

Se il documento riguarda dati personali, questo va eliminato solo ed esclusivamente attraverso il distruggi-documenti. In caso di dubbio, è sempre meglio utilizzare il distruggi-documenti.

L'eventuale documentazione cartacea che può essere riciclata va prima valutata con il criterio indicato per i documenti da eliminare (non devono contenere dati personali).

Fotografie e filmati

È vietato l'uso all'interno degli ambienti di lavoro di dispositivi per produrre fotografie, filmati o registrazioni di ogni tipo, salvo espressa autorizzazione del Responsabile di Area. Fare fotografie, filmati e registrazioni di ogni tipo è vietato sia con apparecchiature personali che con apparecchiature di Persico.

Cambio di mansione/attività/incarico di lavoro

Eventuali documenti contenenti dati personali contenuti all'interno della propria cassetiera e/o armadio e pertinenti a mansioni/attività/incarichi che non verranno più svolte in futuro vanno consegnati al Responsabile di Area (inclusi eventuali supporti di memorizzazione esterna).

Smart Working

In occasione dell'attivazione della prestazione di lavoro in modalità da remoto (smart working), il dipendente/collaboratore è tenuto a seguire prioritariamente le policy e le raccomandazioni dettate dall'organizzazione.

In particolare, il dipendente è tenuto a:

- utilizzare i sistemi operativi per i quali l'organizzazione garantisce il supporto;
- effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo;
- assicurarsi che i software di protezione del sistema operativo (Firewall, Antivirus, etc.) siano abilitati e costantemente aggiornati;
- assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dall'organizzazione;
- non installare software proveniente da fonti/repository non ufficiali;
- bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico (screen saver) quando ci si allontana dalla postazione di lavoro;
- non cliccare su link o allegati contenuti in e-mail sospette;
- utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette (no Wi-Fi libere ed aperte);
- collegarsi a dispositivi mobili (pen-drive, hdd-esterno, etc.) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dall'organizzazione);
- porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel luogo di prestazione dell'attività lavorativa fuori sede;
- conservare e tutelare i documenti eventualmente stampati alla conclusione della prestazione lavorativa giornaliera
- evitare l'uso dei social network, o altre applicazioni social facilmente hackerabili;
- evitare di rivelare al telefono informazioni di carattere personale.

Violazioni e sanzioni disciplinari

Qualora si ravvisassero violazioni di una o più delle prescrizioni definite nel presente documento, potranno essere avviate procedure per l'attribuzione di sanzioni disciplinari.