Policy aziendale

Rev. 1.4
Del: 22/04/2022

Posta elettronica aziendale

Lo scopo

La società, per esclusive finalità lavorative/professionali, può mettere a disposizione mezzi informatici/telematici e l'accesso a Internet, quali strumenti di ricerca, archiviazione e lavoro, nonché strumenti di comunicazione, e di condivisione di informazioni strettamente lavorativi (es. posta elettronica, accesso alla rete aziendale da remoto, etc…).

La **CORE INFORMATICA S.R.L.** ha deciso, quindi, di adottare la presente Policy Aziendale per l'utilizzo degli strumenti aziendali al fine di fornire un quadro preciso di indicazioni ai Lavoratori, e a tutti gli altri Destinatari, in merito alla modalità di funzionamento degli Strumenti Aziendali loro assegnati o da essi comunque utilizzati, e dunque codificare il set di regole di comportamento da rispettare per un corretto utilizzo dei predetti Strumenti Aziendali, onde evitare problemi, disservizi e maggiori costi (di manutenzione o di altro tipo) ovvero rischi e/o minacce alla sicurezza dei sistemi e/o dei dati in essi contenuti, con particolare riguardo ai dati personali e/o al patrimonio della **CORE INFORMATICA S.R.L.**.

L'utilizzo degli Strumenti Aziendali deve sempre ispirarsi ai principi di massima diligenza, buona fede e correttezza; principi, questi, che devono costantemente uniformare e caratterizzare la condotta generale ed i singoli comportamenti di tutti i soggetti autorizzati all'uso dei predetti Strumenti.
La Policy Aziendale, pertanto, è finalizzata anche ad evitare che i Destinatari possano esporre sé stessi e/o la **CORE INFORMATICA S.R.L.**a sanzioni pecuniarie o penali, derivanti da un uso scorretto o illecito degli Strumenti Aziendali, nonché esporre la **CORE INFORMATICA S.R.L.** a una serie conseguenze pregiudizievoli, in relazione al suo patrimonio e/o alla sua immagine.

Ulteriore scopo della Policy Aziendale è disciplinare le condizioni ed i limiti per il legittimo utilizzo di ogni altro strumento e/o dispositivo informatico e/o telematico messo a disposizione dalla **CORE INFORMATICA S.R.L.**, al fine di diffondere una cultura della sicurezza che concorra al conseguimento ed al mantenimento dei più alti livelli qualitativi dei servizi resi.

Scopo della Policy Aziendale è anche quello di recepire e dare attuazione alle disposizioni normative e ai principi previsti dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito "GDPR"), nonché dei Provvedimenti emanati dal Garante per la protezione dei dati personali (di seguito "Garante") al fine di garantire la protezione dei dati personali trattati mediante tali strumenti, nonché la salvaguardia del patrimonio informativo aziendale, gli standard

qualitativi dei servizi resi ed il know-how della **CORE INFORMATICA S.R.L.** (costituito da dati, notizie ed informazioni di carattere strettamente riservato e confidenziale) da parte di coloro che agiscono nella struttura della**CORE INFORMATICA S.R.L.**o che prestano la propria attività in favore della stessa anche al di fuori della sua struttura, indipendentemente dalla natura contrattuale del rapporto professionale in corso.

Pertanto, nel rispetto delle previsioni di cui agli artt. 4 e 8 della Legge 20 maggio 1970, n. 300 (di seguito "Statuto dei Lavoratori"), la **CORE INFORMATICA S.R.L.**intende anche disciplinare, con il Regolamento, le modalità di raccolta ed utilizzo delle informazioni e dei dati trattati tramite gli Strumenti Aziendali, informando circa l'esercizio dell'eventuale potere disciplinare della **CORE INFORMATICA S.R.L.**nei confronti del Personale, qualora si verificasse ed accertasse - secondo le procedure e nel rispetto delle garanzie e tutele oggetto delle previsioni che seguono - un uso improprio e/o non autorizzato degli Strumenti Aziendali assegnati e/o in loro dotazione.

Campo di applicazione

La Policy Aziendale - Gestione posta elettronica aziendale - si applica a tutti i soggetti che utilizzano gli Strumenti Aziendali, tra cui, a mero titolo esemplificativo e non esaustivo:

a) lavoratori subordinati, nonché in distacco o in somministrazione, in ogni caso senza distinzione di durata, orario, ruolo, funzione e/o livello (ivi inclusi i dirigenti) e/o modalità di svolgimento della prestazione, compresi anche eventuali lavoratori in cd. "smart working" (di seguito anche solo il "Personale");
b) collaboratori, a prescindere dal rapporto contrattuale intrattenuti.

Tutti i soggetti sopra elencati saranno di seguito, congiuntamente, indicati come "Personale".

La Policy costituisce anche espressione dei doveri di correttezza comportamentale e diligenza contrattuale e costituisce parte integrante del complessivo sistema normativo aziendale.

La presente Policy si applica altresì a qualunque soggetto che si trovi in possesso di specifiche credenziali di autenticazione per l'accesso alla rete informatica utilizzata dalla **CORE INFORMATICA S.R.L.** o che comunque utilizzi, a qualsiasi titolo, anche in via temporanea, gli Strumenti Aziendali, in qualunquesede e/o ufficio, al fine di proteggere e mantenere riservati i dati trattati e di evitare che, attraverso l'eventuale utilizzo di tali strumenti la **CORE INFORMATICA S.R.L.** possa essere esposta a rischi.
I soggetti di cui sopra, unitamente al Personale, saranno di seguito congiuntamente indicati come "Destinatari".

DISPOSIZIONI PER IL PERSONALE DIPENDENTE

La posta elettronica, messa a disposizione da **CORE INFORMATICA S.R.L.** a favore dei Destinatari all'uopo autorizzati, rappresenta uno strumento di esclusiva proprietà aziendale per lo svolgimento di attività lavorative/ professionali. Tali indirizzi di posta elettronica sono di esclusiva proprietà aziendale e i Destinatari all'uopo autorizzati condivideranno la responsabilità del loro utilizzo.

Per una corretta fruizione del servizio di posta elettronica aziendale, che tuteli i Destinatari e la **CORE INFORMATICA S.R.L.** , devono essere rispettate le seguenti regole:

- è necessario fare attenzione alla posta ricevuta. Nel caso di mittenti sconosciuti o messaggi insoliti, di dubbia autenticità o provenienza e/o con contenuti non attinenti al lavoro svolto, per non correre il rischio di essere infettati da virus e/o malware e/o di essere vittima di Phishing, è necessario verificare il sorgente/intestazione/header del messaggio ricevuto e in caso di dubbio occorrerà contattare immediatamente il personale della Funzione IT. A seguito verifica con individuazione di possibili minacce si deve procedere conla cancellazione dei messaggi senza aprirli. In particolare, non dovranno essere aperti documenti con estensioni diverse da quelle comunemente utilizzate e autorizzate (.doc, .xls, .ppt, .pdf) e/o con nomi “sospetti” e/o "anomali". Qualora, in allegato ad un'e- mail, vi fossero file sospetti o anomali (estensione .exe anche contenuti in file .zip) è necessario accertarsi preventivamente del loro contenuto, verificando il mittente del messaggio e contattando il mittente medesimo per assicurarsi della trasmissione o per informarlo di una possibile problematica sui propri sistemi informatici (es. la presenza di malware che effettua invii a sua insaputa). Non bisogna pigiare link di provenienza dubbia o incerta senza averli verificati in quanto con il click del mouse su un collegamento malevolo all’interno di una mail, è possibile infettare le postazioni di lavoro in modo irreparabile. Sono predisposte specifiche guide operative messe a disposizione per aiutare i Destinatari nella verifica. Per precauzione, contattare immediatamente il personale della Funzione IT. In ogni caso è obbligatorio controllare tutti i file in allegato prima del loro utilizzo e non eseguire download di file eseguibili. Il Lavoratore deve prestare particolare attenzione a filedi tipo archivio compresso (.zip, .rar, .tar, .targz, .gz, etc…) che dovessero essere allegati a mail in quanto possono contenere file eseguibili dannosi di tipo malware. In caso di dubbi, contattare immediatamente il personale della Funzione IT;
- accertarsi che gli eventuali allegati dei propri messaggi non eccedano la dimensione massima prevista per il destinatario;
- inviare allegati solo nei formati più usati: ad es. *.txt, *.rtf, *.doc, *.ppt, *.xls, *.pdf, *.gif, *.tif;

- non è consentito inviare o memorizzare messaggi di natura oltraggiosa, violenta, volgare e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum, social network o mailing-list, salvo diversa ed esplicita autorizzazione da parte della **CORE INFORMATICA S.R.L.**. L'iscrizione ad una mailing list o a servizi simili (chat, forum, social network, ecc.) è consentita solo se funzionale all'attività aziendale e previa autorizzazione del proprio responsabile;
- non è, altresì, consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per inviare messaggi di tipo umanitario, sociale o di solidarietà, salvo diversa ed esplicita autorizzazione rilasciata dal proprio responsabile;
- non è consentito utilizzare la posta elettronica per finalità che esulano dall'espletamento delle mansioni affidate a ciascun dipendente;
- non è consentito creare, archiviare o spedire messaggi pubblicitari o promozionali in nessun modo connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto;
- non è consentito inviare messaggi in risposta a richieste di adesione a programmi di catene di e-mail, indipendentemente dalle finalità presunte;
- non è consentito scaricare sulla propria area di server o sulle risorse condivise in rete file allegati a messaggi di posta elettronica di caselle diverse da quelle assegnate all'utilizzatore;
- non è consentito utilizzare share di rete aziendali (cartelle condivise sia d'ufficio che personali) per archiviare file personali non attinenti con l'attività lavorativa;
- la posta elettronica non deve essere utilizzata per ricevere, memorizzare o spedire materiale che violi le norme sul diritto d'autore o proprietà industriale (copyright, marchi, ecc.);
- quando possibile, inviare gli allegati ai messaggi rivolti a destinatari esterni alla **CORE INFORMATICA S.R.L.** in un formato compresso (*.zip, *.rar), al fine di ottenere un messaggio di dimensioni più contenute possibile, riducendo così il rischio di un mancato recapito a causa delle sue dimensioni eccessive;
- sempre per ragioni di contenimento della dimensione dei messaggi, è fortemente sconsigliato inserire immagini o altri file multimediali nel loro corpo;
- qualora si renda necessario inviare immagini per motivi d'ufficio (es. per inviare la cattura dello schermo di una maschera di un gestionale al fine di documentare una anomalia/errore di un servizio applicativo/programma software) si devono rendere inintelligibili eventuali i dati personali presenti (es. utilizzando strumenti grafici a bordo

delle PdL come paint o gimp); possono rimanere codici identificativi al fine di dare l'informazione minima per poter identificare la posizione da analizzare;

- Gli utenti sono tenuti a mantenere in ordine la propria casella di posta elettronica, cancellando documenti inutili ed e-mail non necessarie, in modo tale da razionalizzare l'impiego delle risorse informatiche e tecnologiche e archiviando localmente la posta che non è necessario mantenere sul server per consultazione online;
- è definito un limite massimo delle dimensioni di una casella postale;
- Qualora si raggiunta la soglia massima delle dimensioni della propria casella di posta elettronica, all'utente sarà notificato dal sistema di posta elettronica il superamento di tale soglia. Superato il limite massimo, l'invio di nuovi messaggi sarà automaticamente inibito e l'utente dovrà necessariamente procedere alle operazioni previste per ripristinare la funzionalità della propria casella postale, quindi contattare il Responsabile Privacy interno della **CORE INFORMATICA S.R.L.**;
- l'invio di messaggi tramite indirizzamenti collettivi (dipendenti, macroaree, ecc.) o individuali di tipo massivo (elenco alfabetico o non della totalità dei dipendenti o estratti) è permesso esclusivamente ai soggetti espressamente autorizzati dal Titolare.

Ogni comunicazione interna/esterna, che deve essere inviata/che è ricevuta, che abbia contenuti rilevanti o contenga impegni per la **CORE INFORMATICA S.R.L.** deve essere autorizzata o visionata dal superiore gerarchico.

E' fatto espresso divieto di usare la casella di posta elettronica aziendale per ragioni e/o finalità personali e di inoltrare, in qualunque modo, verso eventuali strumenti di web mail personali, messaggi ricevuti sulla casella di posta elettronica aziendale e/o dati, documenti e/o informazioni della **CORE INFORMATICA S.R.L..**

Infine, si informa che in alcuni casi particolari, su esplicita richiesta delle Autorità competenti (Guardia di Finanza, Autorità Giudiziaria, ecc.), le e-mail memorizzate nei server della **CORE INFORMATICA S.R.L.** potrebbero essere eventualmente rese note e consegnate alle stesse.

Nei casi di assenza programmata, il Personale dovrà utilizzare il sistema di risposta automatica disponibile (attualmente sia da client di posta installato sul PC sia tramite webmail) della posta elettronica aziendale indicando almeno la data di inizio del periodo di assenza, la data di ripresa del servizio e, al fine di garantire la continuità del servizio, ove possibile, dovrà indicare il nominativo di un altro utente a cui potrà essere inviata, in copia conoscenza, la propria corrispondenza elettronica. In caso di prolungata assenza o in situazioni di emergenza, i Destinatari

potranno attivare tale dispositivo di risposta automatica in riferimento ai rispettivi indirizzi di posta elettronica aziendale.

In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, il Personale potrà delegare un'altra persona (fiduciario) a verificare il contenuto dei messaggi e ad inoltrare alla **CORE INFORMATICA S.R.L.** quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

In ogni caso, al fine di assicurare la disponibilità per la **CORE INFORMATICA S.R.L.** del contenuto della casella di posta elettronica aziendale, in caso di improvvisa o prolungata assenza (es. malattia) dei Destinatari o di un loro impedimento, l'accesso alla predetta casella di posta elettronica aziendale potrà essere effettuato dal personale autorizzato o dal Responsabile privacy interno su esplicita e motivata richiesta scritta del Titolare. Sarà cura del personale autorizzato o dal Responsabile Privacy interno a realizzare dei report di tali attività al fine di informare il Destinatario interessato alla prima occasione utile.

Nel caso di cessazione del rapporto di lavoro (subordinato/ di collaborazione o somministrazione, ecc.), al fine di consentire la continuità lavorativa la **CORE INFORMATICA S.R.L.**, previa immediata disattivazione dell'account di posta elettronica aziendale, potrà attivare un sistema di risposta automatica che informi i mittenti delle e-mail della disattivazione dell'account di posta elettronica aziendale /o della cessazione del rapporto di lavoro, invitandoli a contattare altro dipendente/funzione aziendale.

Una volta disattivato l'account di posta elettronica, copia dei messaggi di posta elettronica sarà conservata sul server centrale e/o sui backup della **CORE INFORMATICA S.R.L.**, entro i termini previsti dal presente Regolamento e/o dalla Retention Policy, salvo che vi siano elementi che inducano la **CORE INFORMATICA S.R.L.** stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di difesa di un diritto in sede giudiziaria), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

Policy aziendale

Rev. 1.4
Del: 22/04/2022

PASSWORD POLICY

La gestione delle credenziali di accesso

Obiettivi generali

La protezione delle credenziali di accesso rappresenta uno dei principi fondamentali della sicurezza delle informazioni, in particolare la creazione e la gestione delle password che costituiscono la principale contromisura agli accessi non autorizzati.

Visto quanto previsto dal regolamento europeo UE 2016/679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, occorre definire misure di protezione adeguate ed idoneeper il trattamento e la tutela dei dati personali gestiti dall'organizzazione.

Il presente documento ha lo scopo di definire una procedura - la password policy
- che stabilisca i criteri per la creazione, l'utilizzo, la conservazione e la gestione delle credenziali di autenticazione fornite agli utenti per l'accesso ai servizi informatici erogati.

In generale, i servizi informatici utilizzati dall'organizzazione individuano, come strumento di accesso per gli utenti, un sistema di autenticazione (e di autorizzazione) basato su credenziali di accesso.
Esso consiste in un codice per l'identificazione dell'utente ("*username*" o "*nome utente*"), associato ad una parola chiave riservata ("*password*") conosciuta esclusivamente dal solo utente. I due elementi, uniti insieme, costituiscono la credenziale di accesso ("*account*" o *"utenza"*) così come definito dalla normativa vigente in tema di dati personali.

Campo di Applicazione

La password policy si applica a tutti i servizi informatici centrali, gestionali ed applicativi, compresi quelli web, alle postazioni di lavoro, alla rete lan, al servizio di posta elettronica e a tutte le applicazioni e risorse informatiche che prevedono un sistema di autenticazione per l'accesso.

Responsabilità degli amministratori di sistema

Gli amministratori di sistema devono proteggere la riservatezza e l'integrità delle password sui sistemi da loro gestiti e configurare i servizi informatici, forzando l'applicazione ove tecnicamente possibile, per soddisfare i requisiti della presente password policy.

Lo *username* viene assegnato, salvo diverso avviso, esclusivamente dall'amministratore del servizio (o amministratore del sistema) o da un suo delegato. La password viene gestita, dopo la sua prima assegnazione da parte dell'amministratore, esclusivamente dall'utente, con l'eccezione dei casi in cui ricorrano necessità di carattere tecnico-organizzative.

Il codice identificativo, una volta assegnato ad un utente, non potrà più essere riassegnato ad altri soggetti, nemmeno in tempi successivi, proprio per poter garantire un'archiviazione e storicizzazione delle utenze.

Le credenziali di accesso non utilizzate da almeno 6 (sei) mesi dovranno essere disattivate (a meno che non siano state preventivamente autorizzate quali credenziali per soli scopi di gestione tecnica, che prevedono pertanto periodi di inattività anche più lunghi del semestre). Le credenziali devono essere disattivate anche quando l'utente perde il ruolo, la mansione e le qualità che gli consentono di utilizzarle per accedere ai vari servizi (es. dimissioni, licenziamento, trasferimento, cambio di mansioni, sostituzione, ecc.).

Laddove vi sia la ragionevole certezza che l'utenza sia stata utilizzata da persona diversa dal titolare, la stessa dovrà essere cambiata immediatamente dall'utente. In caso di inerzia, tale cambio verrà disposto direttamente dall'amministratore del sistema. Le password di default - come quelle create per i nuovi utenti o assegnate dopo una reimpostazione della password - devono poter essere cambiate dall'utente al primo accesso. Se tecnicamente possibile, tale cambio password deve essere imposto all'utente dal sistema.

Responsabilità degli utenti

Gli utenti si impegnano a rispettare i criteri di creazione, conservazione e gestione delle credenziali di accesso di seguito indicati.

Gli utenti, una volta in possesso delle credenziali, devono cambiare la password al primo accesso rispettando i criteri di seguito descritti, evitando combinazioni facili da identificare. Devono scegliere password univoche, che abbiano un senso solo per l'utente che le sceglie, evitando di usare la stessa password per altre utenze.

La password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona all'interno dell'organizzazione, compresi colleghi, superiori, collaboratori, consulenti, ecc.

Gli utenti devono prestare attenzione a fornire le proprie credenziali di accesso, a rispondere ad e-mail sospette e/o a cliccare sui link durante la navigazione web (o nella mail) al fine di contrastare possibili frodi informatiche (come il phishing, lo spear phishing, il furto d'identità, ecc.).

Ogni utente è responsabile di tutte le azioni e le funzioni svolte dal suo account.

Qualora vi sia la ragionevole certezza che le credenziali assegnate siano state utilizzate da terzi, l'utente dovrà cambiare immediatamente la password.

Per la conservazione sicura delle credenziali di accesso può essere opportuno usare un software di gestione delle password (es. KeePass, LastPass, ecc.) evitando di memorizzarle su fogli di carta, documenti cartacei e file conservati all'interno della postazione di lavoro. Tali software permettono anche di automatizzare il processo di login alle varie applicazioni usate.

Qualora l'utenza venga bloccata a seguito della scadenza della password oppure sia necessario modificare la password perché dimenticata ovvero a fronte di qualsiasi altra motivazione, l'utente deve utilizzare i servizi self-service di reimpostazione o di cambio password (ove disponibili) oppure contattare il servizio IT interno o l'amministratore di sistema.

Requisiti tecnici per la creazione e gestione delle password

Come regola generale, la password deve essere ragionevolmente complessa e difficile da individuare e/o ricavare.

Nei limiti tecnici consentiti dai sistemi, la password:

1) deve essere di lunghezza non inferiore ad 8 caratteri oppure, nel caso in cui il sistema non lo dovesse prevedere, di lunghezza pari al massimo consentito;
2) deve essere obbligatoriamente cambiata al primo utilizzo e successivamente almeno ogni 6 (sei) mesi;
3) deve contenere, salvo limitazioni imposte dai sistemi, un mix di caratteri tra numeri, caratteri alfabetici in maiuscolo e minuscolo, e caratteri speciali (*es. huTR@@028*);
4) deve essere sempre diversa da almeno le ultime 4 precedentemente utilizzate;
5) non deve presentare una sequenza di caratteri identici o gruppi di caratteri ripetuti;
6) deve essere nota esclusivamente all'utilizzatore e non può essere assegnata e/o comunicata ad altri;
7) non deve contenere riferimenti agevolmente riconducibili all'utente o ad ambiti noti;
8) non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere) o che si riferiscano ad informazioni personali;
9) non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet.

Ove tecnicamente possibile, i requisiti di cui ai punti da 1) a 5) devono essere imposti da meccanismi automatici del sistema.

Per motivate necessità di urgente accesso alle informazioni, in caso di impedimento del titolare delle credenziali, la password può essere annullata e sostituita dagli amministratori di sistema con una nuovapassword.

In questo caso la nuova password dovrà essere consegnata dall'amministratore di sistema all'utente, il quale dovrà modificarla al primo accesso.

Policy aziendale

Rev. 1.4
Del: 22/04/2022

CLEAN DESK POLICY

Obiettivi generali

La “clean desk policy” è un vero e proprio insieme di regole che aiuta a tenere la scrivania pulita ma soprattutto in ordine e quindi libera da tutti gli oggetti e da tutti i documenti non necessari in un determinato momento ed ha come obiettivo primario la protezione dei documenti.

Se da un lato questa politica consente di proteggere i dati trattati, dall’altro contribuisce ad aumentare la produttività visto che il disordine ha un effetto negativo sulla capacità di concentrarsi che a sua volta incide sia sulla capacità di elaborare le informazioni, riducendola, sia sullo stress, aumentandolo.

Campo di Applicazione

Tale procedura si applica su tutti i documenti cartacei presenti sulla scrivania o comunque prodotti da supporti nelle aree di lavoro (p.e. scanner, fotocopiatrici, lavagne)

Responsabilità degli utenti (lavoratori ed ospiti)

Tale politica prevede che il lavoratore durante le pause o quando termina il lavoro non debba mai lasciare sulla scrivania documenti riservati, per evitare che il personale non autorizzato possa consultarli. È quindi preferibile creare uno “spazio d’azione” sulla propria scrivania ovvero organizzare i documenti che si usano frequentemente ai fini lavorativi e conservare quelli non indispensabili.

Informativa agli utenti

La Società si impegna a rappresentare, anche a mezzo informativa interna, le misure adottate e le raccomandazioni a tutti gli utenti delle proprie stazioni di lavoro.

Policy aziendale

Rev. 1.4
Del: 22/04/2022

DEVICE USE POLICY

Obiettivi generali

L'uso dei dispositivi mobili comporta un rischio non trascurabile considerando che gli stessi sono di frequente connessi alla rete aziendale e quindi non è predeterminabile la modalità con cui i dati contenuti vengono scambiati, né si conosce il livello di protezione dei dispositivi connessi; pertanto risulta necessario prestare particolare attenzione alla promiscuità dell'uso (fini aziendali e personali); sul medesimo device potremotrovare – p.e. – scambi di messaggi aziendali e foto personali di famiglia.

Campo di Applicazione

La device use policy si adotta per proteggere i dati contenuti nei dispositivi mobili (telefoni cellulari, smartphone, computer portatili, chiavette USB etc.).

Responsabilità degli utenti (lavoratori ed ospiti)

Tale politica prevede che al lavoratore venga opportunamente indicato l'uso strettamente riservato alle attività di lavoro dei device. L'uso promiscuo - tuttavia - è ricorrente e per certi versi deve essere tollerato. Si pensi ad esempio all'uso del proprio telefonino anche ai fini lavorativi o all'uso di una "chiavetta" aziendale per scaricare atti o documenti personali.

Responsabilità del titolare del trattamento

Una buona politica aziendale potrebbe prevedere che il titolare del trattamento si attivi per:

- consegnare i dispositivi rilasciando raccomandazioni scritte sull'utilizzo;
- specificare che il bene in uso è di proprietà dell'azienda e – se possibile – marcare lo stesso;
- creare un registro contenente il codice identificativo di ogni dispositivo;
- ricorrere a protezioni di tipo criptografiche, quando disponibili;
- riservarsi (a cura del servizio IT) la possibilità di richiedere il device per testarne integrità e assenza di dati non pertinenti al lavoro, estranei o comunque inopportuni;
- effettuare un backup in modo tale da archiviare, e quindi custodire, i dati.

È inoltre consigliabile proteggere ogni dispositivo mobile con una parola chiave sicura - diversa da quella usata per accedere ad altri apparati utilizzati in azienda - modificata ogni 15 giorni, creare reti di comunicazione

chiuse così da rendere i dati accessibili solo a determinate persone e stabilire quali dati personali trattate ovvero distinguere i dati professionali, di cui il datore di lavoro ne è titolare, dai dati personali del lavoratore.

CLOSE DOOR POLICY

Obiettivi generali

Lasciare la stanza in cui si lavora incustodita è un gesto frequente ma poco accorto.

A parte la ovvia impossibilità – ogni volta – di usare l'attenzione di lasciare sgombra la scrivania da documenti facilmente consultabili o a rischio sottrazione, la chiusura della porta risponde ad una esigenza di tutelare i dati "sparsi" ovunque oltre che di preservare il lavoro svolto.

Il rischio di rendere accessibile l'ufficio, rende peraltro possibile la sottrazione di beni, documenti e valori personali. La confidenzialità e la fiducia verso i colleghi non giustifica il rischio che si corre soprattutto se i locali sono frequentati da estranei, visitatori occasionali od anche abituali.

Campo di Applicazione

La close door policy si adotta per proteggere da sottrazione o consultazione di documenti, informazioni e dall'uso di strumenti custoditi all'interno di un ufficio e più genericamente per inibire l'accesso da parte di soggetti non autorizzati.

Infine tale policy limita il rischio di furti di oggetti, valori e documenti personali che inevitabilmente il lavoratore porta con sé.

Tali concetti vanno rafforzati per i locali che maggiormente detengono e gestiscono dati di maggiore delicatezza e complessa articolazione (p.e. Uffici del Personale, Ufficio Progettazione, Ufficio Commerciale).

Responsabilità degli utenti (lavoratori ed ospiti)

Al lavoratore viene spiegato che, se la porta ha una chiave, essa va utilizzata anche durante il turno di lavoro e non magari solo al termine della giornata.

La sistemazione in stanza con altri colleghi o collaboratori giustifica, tuttavia, che non si proceda a serrare con chiave la bussola e consiglia la dotazione di una porta con apertura elettrica a scatto che consenta agli esterni di accedere previo annuncio con l'uso di un campanello o col più tradizionale colpo di nocche sulla porta.

Responsabilità del titolare del trattamento

Una buona politica aziendale potrebbe prevedere che il titolare del trattamento si attivi per:

- consegnare a tutti i dipendenti abilitati una copia della chiave di accesso al proprio ufficio marcandola univocamente (p.e. con la matricola del dipendente);
- specificare che l'accesso è consentito negli orari di lavoro e che la chiave va sempre portata con sé sotto la propria responsabilità;
- gestire un elenco dei detentori di chiave e provvedere ad eventuali sostituzioni in caso di denunciato smarrimento, evitando duplicazioni laddove si valuti il rischio che lo smarrimento possa riferirsi a sottrazione nel qual caso si provvederà a sostituire la serratura stessa;
- verificare periodicamente che tutti gli autorizzati abbiano la propria chiave e procedere alla sostituzione di serratura in caso di frequenti o numerosi smarrimenti registrati in un arco di tempo di osservazione (dai 3 ai 6 mesi, a seconda dell'indice di frequentazione da parte di estranei dei locali interessati e considerando altresì il turn-over di dipendenti, stagisti e collaboratori).
- ritirare la chiave del lavoratore/collaboratore che lascia l'azienda o che semplicemente cambia ufficio, verbalizzando e facendo sottoscrivere allo stesso una dichiarazione in cui questi confermi di non avere operato riproduzioni della chiave stessa;
- laddove economicamente accettabile installare meccanismi di apertura a mezzo smart card o tesserino personale istituendo procedure di cautela equivalenti a quanto sopra detto per la chiave tradizionale.

Policy aziendale

Rev. 1.4
Del: 22/04/2022

CLOSE LOCKER POLICY

Obiettivi generali

L'uso di armadi a chiave tutela dati ed informazioni riservate, rafforzando la custodia anche all'interno di uffici presidiati da chiave o da accessi limitati e vigilati.

L'armadio o la cassaforte aggiungono peraltro una ulteriore protezione fisica da agenti esterni (allagamenti, incendi, etc.) ed inibiscono o comunque rallentano qualsiasi tentativo di sottrazione di documenti o valori.

La mancata chiusura a chiave (o a lucchetto) di fatto rende quasi inutile il posizionamento, se non per motivi di ordine e pulizia.

Campo di Applicazione

La close locker policy si adotta per proteggere da sottrazione o consultazione di documenti, informazioni e valori custoditi all'interno di un armadio, di una cassaforte o di una cassetta a chiave.

Questa policy limita al massimo il rischio di furti di oggetti, valori e documenti normalmente riservati per l'azienda che ne ha disposto la massima tutela possibile.

Responsabilità degli utenti (lavoratori ed ospiti)

Al lavoratore viene spiegato che la chiave va sempre usata in chiusura anche quando l'apertura del presidio è limitata nel tempo (anche pochi minuti) e ciò al fine di assumere una abitudine che limita l'eventuale distrazione successiva al prelievo di documenti o valori.

Tale cautela va amplificata laddove gli armadi o le cassette si trovano in uffici comuni o in locali di passaggio (corridoi, sale riunioni etc.).

Responsabilità del titolare del trattamento

Una buona politica aziendale potrebbe prevedere che il titolare del trattamento si attivi per:

- consegnare sotto verbalizzazione solo a dipendenti abilitati, con idonea anzianità di servizio e collaudata esperienza, la /le chiave/i di apertura di armadiature destinate a contenere documenti e/o valori la cui custodia è inerente al lavoro dell'incaricato tenutario della chiave stessa;

- specificare il valore intrinseco ed informativo dei documenti e valori custoditi all'assegnatario di chiave;
- specificare che l'apertura del presidio è opportuna solo per comprovata esigenza di servizio e che la esibizione di qualsiasi documento in essa contenuto deve essere compatibile con quanto stabilito dal ruolo o mansione
- specificare che la chiave va sempre portata con sé sotto la propria responsabilità o – più opportunamente - riposta in altro presidio (esempio in cassaforte) sotto la responsabilità di altro dipendente (di regola di rango o responsabilità superiore) e ciò per limitare il rischio di sottrazione o smarrimento fuori dei locali aziendali;
- specificare che qualsivoglia evento legato al possesso di chiavi (furto, smarrimento anche momentaneo) o al presidio (forzatura, insolito riscontro di apertura, etc.) va immediatamente riferito alla Direzione aziendale o comunque al proprio superiore, senza ritardo e – in caso di impossibilità – denunciando ad Autorità competente (Polizia di Stato, Carabinieri …);
- specificare all'incaricato che la inventariazione dei documenti detenuti sotto chiave è norma per chi è responsabilizzato di presidi a chiave e, in assenza di specifica od oggettiva impossibilità di procedervi, risulta necessaria la massima collaborazione al fine di riscontrare sottrazioni o alterazioni di documenti o valori detenuti;
- gestire un elenco dei detentori di chiave e provvedere ad immediata sostituzione in caso di denunciato smarrimento, provvedendo alla sostituzione della serratura stessa;
- verificare periodicamente che tutti gli autorizzati detengano opportunamente le chiavi a loro assegnate;
- procedere alla sostituzione di serratura in caso di prolungata assenza dell'addetto tenutario, quando il lavoratore/collaboratore lascia l'azienda e quando si sono verificati furti, forzature o episodi di perdita di documenti o valori senza esito delle responsabilità;
- vietare espressamente la duplicazione delle chiavi di armadi ed altri presidi di custodia;
- laddove economicamente accettabile installare via via presidi di crescente sicurezza, con l'avvento di nuove tecnologie (es. sostituire casseforti con combinazione elettronica in luogo di casseforti a chiave tradizionale oppure armadiature blindate in luogo di quelle tradizionali);
- ottenere sempre garanzie dai costruttori circa il grado di sicurezza dei presidi installati e correlarne la sicurezza al valore e/o alla significatività dei dati ed informazioni contenute.

Infine, si invita il personale dipendente, a comunicare tempestivamente il Titolare o il Referente del Sistema Privacy aziendale- in caso di violazione di dati personali di che comporta – accidentalmente o in modo illecito – la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità dei dati personali.

CORE INFORMATICA S.R.L.
Ivrea (TO), 22.04.2022