

Oggetto: Policy Protezione dei dati e sull'utilizzo degli strumenti e attrezzature informatiche, della telefonia mobile, della posta elettronica aziendale e internet

Versione: aggiornamento n. 05 del 24 gennaio 2024

Allegato 1 alla Circolare 29 2019

INDICE

PREMESSA	3
1. Normativa di riferimento	4
Campo di applicazione	4
Glossario	5
POLICY SULL'UTILIZZO DEGLI STRUMENTI E ATTREZZATURE INFORMATICHE, DELLA TELEFONIA MOBILE, DELLA POSTA ELETTRONICA AZIENDALE E INTERNET	7
OBBLIGHI	7
Obblighi della Società	7
Obblighi per i Dipendenti	8
PC Desktop (postazione fissa)	8
PC Laptop (portatili)	9
Telefoni cellulari - smartphones	10
Palmari e tablet	12
Utilizzo di altre attrezzature elettroniche aziendali	13
Dispositivi e supporti di memoria rimovibile e/o portatile	13
GESTIONE DELLA USERID E PASSWORD	13
Caratteristiche della password	14
RETE TELEMATICA INTERNA AZIENDALE (MPLS)	15
INTERNET - ACCESSO e NAVIGAZIONE	15
Accesso alla rete aziendale tramite VPN	16
AUDITING AZIENDALE e ORGANISMO DI VIGILANZA	17
Audit aziendale	17
Organismo di Vigilanza	17
POSTA ELETTRONICA ORDINARIA AZIENDALE (PEO)	17
Generalità	17
Account di posta elettronica	17
Cambio della password della posta elettronica	18
Allegati di posta	18
Spazio di archiviazione della casella di posta - backup	18
Mail Store	19
Messaggio per assenza	19
Sospensione/disattivazione di account di posta elettronica	19
Posta Elettronica Certificata (PEC)	20
SPAM	20
Invio massivo di messaggi di posta	20
Backup della posta elettronica	20



Amministratore di Sistema della posta elettronica	20
VIRUS INFORMATICI E ANTIVIRUS	21
SALVATAGGIO DEI DATI - BACKUP	21
VERIFICHE DA PARTE DELL'AZIENDA E PRINCIPIO DI PERTINENZA E NON ECCEDENZA	22
ASPETTI DI PRIVACY PER IL DIPENDENTE	22
SANZIONI	23



PREMESSA

La Premessa è parte integrante della presente Policy.

La presente Policy coinvolge tutte le Società facenti oggi parte del Gruppo Mondialpol: Vedetta 2 Mondialpol S.p.A., Vigilanza Umbra Mondialpol S.p.A., Logica Infoservice s.r.l., d'ora in avanti chiamate anche "Mondialpol" o "Società" o "Azienda".

Vedetta 2 Mondialpol S.p.A., per sua peculiare natura e per motivi strategici, fornisce alle Società e ai Dipendenti, alcuni o tutti i seguenti servizi:

- interconnessione tra le Sedi;
- connessione internet;
- servizio di PEO;
- gestione PEC;
- gestione dei contratti del servizio di telefonia mobile;
- gestione dei contratti del servizio di telefonia fissa;
- gestione dei contratti del servizio di telefonia VoIP.

Mondialpol si caratterizza per l'elevato uso della tecnologia informatica che da un lato ha consentito l'introduzione di innovative tecniche di gestione dell'impresa, dall'altro ha dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti dall'Azienda ai Dipendenti per lo svolgimento delle proprie mansioni.

La progressiva e capillare diffusione delle tecnologie informatiche, e in particolare dell'accesso alla rete Internet, può esporre la Società a numerosi rischi, sia di carattere patrimoniale che penale, creando problemi alla sicurezza interna delle informazioni sensibili per il core business aziendale, e alla sua immagine pubblica.

In questo senso viene fortemente sentita dai vertici aziendali, la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei Dipendenti, e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'Azienda stessa a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice Civile e dal CCNL.

I controlli preventivi e continui sull'uso degli strumenti informatici in azienda, devono garantire tanto il diritto dell'Azienda di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro il cui utilizzo personale è precluso, quanto il diritto del Dipendente a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza e alla dignità come sancito dallo Statuto dei Lavoratori e dal Regolamento UE 679/2016 sulla tutela dei dati personali.

Il Regolamento di seguito riportato viene incontro a tali esigenze, disciplinando le condizioni per il corretto utilizzo degli strumenti informatici da parte dei Dipendenti, in particolare alla luce degli obblighi previsti dal Regolamento UE 679/2016, relativamente all'adozione delle misure minime di sicurezza per il trattamento dei dati personali.

Qualunque soggetto, anche non Dipendente, che a qualsiasi titolo sia abilitato all'accesso e/o all'utilizzo dei sistemi e/o degli apparati elettronici della Società, è tenuto alla massima riservatezza in merito alle loro



caratteristiche e contenuti, al loro metodo di funzionamento, e alle misure di sicurezza adottate per la loro protezione.

I destinatari della presente sono tenuti a trattare le informazioni esclusivamente per le finalità e con le modalità connesse alle proprie responsabilità e mansioni, nonché a non diffondere in alcun caso le stesse oltre la cerchia dei soggetti sopra riportata.

La presente disposizione viene resa pubblica attraverso: extranet (Callisto), intranet, invio di circolare email a tutti gli utenti della posta elettronica aziendale, affissione in luogo accessibile a tutti; verrà altresì consegnata al momento dell'assunzione a ciascun Dipendente che utilizzi sistemi informativi o apparecchiature elettroniche di proprietà di Mondialpol. Con tali procedure si intendono soddisfatte le condizioni di pubblicazione, informazione e presa di conoscenza.

L'utilizzo degli strumenti informatici e telematici dovrà sempre ispirarsi al principio di diligenza e correttezza, comportamenti questi che sono alla base di un corretto rapporto di lavoro.

La mancata applicazione delle norme contenute in questa Policy costituisce un'inadempienza contrattuale e, pertanto, potrà essere perseguita nei modi e nei termini stabiliti dai contratti e dalle opportune Leggi di settore.

1. Normativa di riferimento

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- Garante per la Protezione dei Dati Personali – “Linee guida del Garante per posta elettronica e internet – 10 marzo 2007”
- L. 20 maggio 1970, n. 300, denominata “Statuto dei Lavoratori”

Campo di applicazione

Lo scopo della presente Policy è quello di fornire le linee guida sulle condizioni minime richieste dalla Società per il corretto utilizzo da parte di ciascun Dipendente, degli strumenti informatici, informativi, della posta elettronica aziendale (PEO e PEC) e della navigazione sulla rete Internet.

Oltre che alle Società del Gruppo, la presente Policy si applica a Consulenti, Società esterne di procacciamento d'affari e/o procacciatori d'affari anche in possesso di partita IVA e iscritti all'Albo ENASARCO, collaboratori, fornitori, business partner, ecc. che trattano informazioni ovvero utilizzano strumenti o sistemi informativi o apparecchiature elettroniche di proprietà di Mondialpol. Anche tutte queste categorie verranno, a mero titolo di comodità, in seguito denominate “Società del Gruppo” o “Dipendenti”, senza quindi per questo intendere ad es. pretesa di qualsivoglia titolo di dipendenza diretta o una presunzione di posizione retributiva diretta da parte di Vedetta 2 Mondialpol S.p.A.



La Società inoltre, in qualità di Titolare del trattamento, ritiene opportuno dotarsi di questa Policy allo scopo di adempiere gli obblighi fissati dal REGOLAMENTO (UE) 2016/679.

La presente Policy è stata predisposta a uso esclusivamente interno della Società e, pertanto, non potrà essere riprodotta, divulgata, copiata, utilizzata e/o altrimenti resa pubblica o essere diffusa a terzi in assenza di una previa autorizzazione scritta, né potrà costituire base informativa e/o valutativa per finalità diverse da quelle per le quali è stata redatta.

Glossario

Titolare del trattamento: è la persona fisica, giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza (Codice in materia di protezione dei dati personali, art. 4). In sostanza il titolare è colui che tratta i dati senza ricevere istruzioni da altri, colui che decide "perché" e "come" devono essere trattati i dati.

Responsabile del trattamento: è la persona fisica o giuridica, l'Autorità Pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

CIO (Chief Information Officer): risponde direttamente al Presidente del CDA; si occupa della direzione strategica dei sistemi informativi in Azienda, in modo che si adattino al meglio ai processi aziendali e costituiscano un elemento di vantaggio competitivo a supporto delle attività di produzione; definisce e/o approva strategie e linee guida per la corretta fruibilità del sistema informativo in Azienda. Segnala alla funzione Audit e/o all'Organismo di Vigilanza, eventuali trasgressioni o anomalie riscontrate o verificatesi, i rimedi adottati nonché le misure poste in atto al fine di evitarne il ripetersi.

CISO (Chief Information Security Officer): si occupa di coordinare le iniziative di sicurezza rispetto ai programmi aziendali e agli obiettivi di business, assicurando che gli asset informativi e le tecnologie siano adeguatamente protetti.

IT Manager: risponde direttamente al CIO e lo informa su tutte le sue attività. È incaricato di monitorare, direttamente ovvero tramite lo Staff IT, i sistemi informativi al fine di individuare un eventuale uso scorretto degli stessi; segnalare prontamente al CIO, Audit e/o all'Organismo di Vigilanza ogni eventuale attività anomala e/o non autorizzata sui sistemi informativi.

Amministratore di Rete: soggetto lecitamente autorizzato ad accedere ai dati sensibili in funzione della sua mansione; risponde direttamente al CIO; sovrintende direttamente o tramite l'IT Manager ovvero lo Staff IT, alla configurazione della Rete Aziendale (MPLS), all'interconnessione tra le Sedi, alla configurazione delle apparecchiature informatiche, al monitoraggio dei flussi dei dati che attraversano i server, i router e gli switch; gestisce direttamente ovvero tramite lo Staff IT, il server della posta elettronica aziendale, il server di archiviazione dello storico della posta elettronica (MailStore) e i firewall. In Mondialpol sono presenti due Amministratori di Rete.

Amministratore di Sistema: soggetto lecitamente autorizzato ad accedere ai dati sensibili in funzione della sua mansione; risponde all'Amministratore di Rete. Sovrintende alla gestione, alla sorveglianza e al monitoraggio dell'uso proprio dei sistemi affidatigli e utilizzati in Azienda, e dei dati ivi contenuti (es: Zucchetti, Knox, Mirage, Intranet, server di dominio ecc...). Gli Amministratori di Sistema sono considerati Responsabili del trattamento.



Staff IT: risponde direttamente al CIO e/o all'IT Manager. Sono i Dipendenti adeguatamente formati e competenti in ambito IT.

Violazione di dati personali: violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Sistema Informativo: per Sistema Informativo si intende, in questa sede, una piattaforma informatica autonoma idonea a elaborare uno specifico processo aziendale. In Mondialpol vengono utilizzati diversi sistemi informativi.

Apparato informatico - attrezzatura informatica: sono tutte quelle apparecchiature, fisse e mobili, in grado di immagazzinare ed elaborare dati, e connettersi a una rete informatica (PC, tablet, smartphones, palmari, GPS/GSM ecc.).

UserID: può essere un nome, un soprannome, un codice o un indirizzo email di autenticazione con cui ci si identifica per accedere a un Sistema Informativo o a un Apparato Informatico.

Password: codice alfanumerico abbinato alla UserID per accedere a un Sistema Informativo o a un Apparato Informatico.

Credenziali: l'insieme di UserID e Password.

Admin: colui che amministra un sistema informativo o un'apparecchiatura informatica; crea, configura, elimina e modifica gli utenti.

Utente: colui che utilizza un sistema informativo o un'apparecchiatura informatica, con accessi definiti.

RPD/DPO: è il Responsabile Protezione Dati (Data Protection Officer). Risponde direttamente al Titolare del Trattamento dei dati.

MPLS: (sempl.) rete informatica geografica privata.

SSO: Single Sign On. Sistema che permette all'utente di autenticarsi con unico login, a più sistemi informativi.



POLICY SULL'UTILIZZO DEGLI STRUMENTI E ATTREZZATURE INFORMATICHE, DELLA TELEFONIA MOBILE, DELLA POSTA ELETTRONICA AZIENDALE E INTERNET

I capi area, capi ufficio, caposervizi, responsabili di funzione, nella loro qualità di responsabili in quanto tali, sono tenuti a:

- informare il personale in merito al corretto utilizzo delle risorse del sistema informativo aziendale, fornendo copia del presente Regolamento, ovvero specificando le modalità ove lo stesso può essere rinvenuto (sito internet aziendale, extranet, intranet);
- assicurarsi che il personale a loro assegnato si uniformi alle regole e alle procedure qui descritte, e riportare di volta in volta, ovvero in sede di relazione annuale, al Responsabile Protezione Dati (RPD o DPO dpo@mondialpol.email), le infrazioni eventualmente commesse dalla propria unità organizzativa, sulle responsabilità nonché in merito ai provvedimenti conseguentemente assunti;
- valutare la necessità di dotare o meno il personale di strumenti informatici (quale anche l'account di posta elettronica), determinare il profilo per l'accesso al sistema informativo, e comunicare all'RPD (dpo@mondialpol.email) eventuali successive variazioni;
- raccogliere e valutare le richieste di accesso del personale loro assegnato, ai sistemi in uso in Mondialpol e ai data base; per nessun motivo i responsabili potranno concedere, al personale loro assegnato, le proprie credenziali di accesso ai sistemi informativi.

Ogni Dipendente e collaboratore a qualsiasi titolo, è personalmente e direttamente responsabile per ciò che concerne:

- il rispetto delle regole di cui al presente Regolamento;
- ogni uso che venga effettuato delle attrezzature informatiche e delle credenziali (account, password e User ID assegnategli) fatto salvo l'eventuale uso improprio delle stesse derivante da fatto non imputabile al Dipendente.

OBBLIGHI

Obblighi della Società

I trattamenti effettuati da Mondialpol si svolgono nell'osservanza dei seguenti principi:

- il principio di necessità, secondo cui, in relazione alle finalità perseguite, i sistemi informativi devono essere configurati riducendo al minimo l'utilizzo di dati personali e di dati identificativi;
- il principio di correttezza, secondo cui le modalità dei trattamenti vengono rese note ai Dipendenti, in modo da scongiurare l'eventuale svolgimento di trattamenti ulteriori rispetto a quelli strettamente connessi all'attività lavorativa ed effettuati all'insaputa o senza la piena consapevolezza dei medesimi;
- il principio del trattamento per finalità determinate, esplicite e legittime, osservando il principio di non eccedenza.

In quest'ottica, Mondialpol tratta i dati dei Dipendenti nella misura meno invasiva possibile, affidando eventuali attività di monitoraggio esclusivamente a quei soggetti opportunamente e lecitamente preposti, ed effettuando eventuali controlli esclusivamente in maniera mirata sull'area di rischio, tenuta in debito conto la normativa sulla protezione dei dati e, se pertinente, il principio di segretezza della corrispondenza.



In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato al principio della trasparenza. Grava quindi sul Datore di Lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette, e in che misura e con quali modalità vengano effettuati i controlli.

La presente Policy ha l'intento di assolvere a quest'obbligo.

Mondialpol, inoltre, ha predisposto tutte le accortezze necessarie affinché i dati personali contenuti nelle postazioni di lavoro informatiche siano protetti contro il rischio d'intrusione tanto dall'esterno (Internet) che dall'interno (rete locale) dall'azione di programmi di cui all'art. 615-quinquies del Codice Penale, attraverso l'utilizzo di idonei strumenti elettronici, mantenuti costantemente aggiornati. Anche i programmi della postazione di lavoro sono costantemente e periodicamente aggiornati al fine di prevenire le vulnerabilità.

Sono state attuate, altresì, le opportune modalità tecniche volte a provvedere al salvataggio dei dati con frequenza almeno settimanale, e sono state previste e adottate le opportune procedure volte a garantire il ripristino dell'accesso alle informazioni o agli strumenti elettronici danneggiati in un arco di tempo non superiore ai 7 (sette) giorni.

Obblighi per i Dipendenti

Di seguito vengono specificati gli obblighi e le norme di condotta obbligatorie per i Dipendenti e per tutti coloro che, in virtù di un rapporto di lavoro, collaborazione o fornitura, trattano informazioni ovvero utilizzano, gestiscono, mantengono o abbiano accesso come Admin o come Utente, a uno o più sistemi informativi o apparecchiature elettroniche e/o informatiche di proprietà di Mondialpol.

PC Desktop (postazione fissa)

Il PC fisso assegnato all'utente è uno strumento di lavoro e deve essere utilizzato secondo criteri di diligenza e correttezza, evitando ogni possibile forma di danneggiamento. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Il PC fisso dato in assegnazione all'utente, permette l'accesso all'MPLS aziendale solo attraverso specifiche credenziali di autenticazione.

Ai fini della corretta custodia del PC fisso:

- il Dipendente è tenuto a utilizzare il PC con la massima diligenza e cura;
- il Dipendente non può spostare e/o installare in autonomia il PC fisso in altro ufficio o fuori dai locali dell'Azienda, salvo previa autorizzazione del Responsabile della Funzione IT e del Responsabile gerarchico. Salvo diversa autorizzazione, lo spostamento del PC fisso deve avvenire tramite l'ausilio del personale tecnico del Servizio IT;
- salvo diverse istruzioni ricevute dal Servizio IT per esigenze di manutenzione, il PC fisso deve essere spento al termine della giornata lavorativa e, in caso di assenze prolungate dall'ufficio, anche al fine di evitare accessi o tentativi di accesso da parte di terzi non autorizzati, di incorrere in potenziali rischi elettrici e per non sprecare risorse energetiche;
- in caso di allontanamento anche temporaneo dalla postazione di lavoro, il Dipendente non deve lasciare il sistema operativo "aperto" (accessibile) con la propria password inserita. Al fine di scongiurare accessi non consentiti, ogni qualvolta ci si allontana dalla propria postazione di lavoro, il Dipendente deve



attivare il salvaschermo con password, o deve bloccare il computer con la combinazione di tasti CTRL+ALT+CANC;

- ove compatibile con l'attività operativa, il sistema sarà configurato dal Servizio IT in modo da oscurare lo schermo e impedire l'accesso dopo 15 minuti di inattività dell'utente. Per ripristinare l'operatività l'utente dovrà reinserire la password personale.

In sintesi il Dipendente deve avere cura di non lasciare il PC incustodito connesso alla rete in quanto si potrebbe verificare un utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In questo caso la responsabilità ricade sull'utente.

Non è consentito l'uso di programmi (applicazioni) diversi da quelli ufficialmente installati dal personale del Servizio IT per conto della Azienda, nè è consentito di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave rischio di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni installate.

L'inosservanza della presente disposizione espone la stessa 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 licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico della Azienda, come disposto dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie e interdittive.

Salvo preventiva espressa autorizzazione del personale del Servizio IT, non è consentito all'utente di modificare le caratteristiche impostate sul proprio PC né procedere a installare dispositivi di memorizzazione esterni (dischi fissi rimovibili, chiavette USB, ecc.), comunicazione o altro (masterizzatori, modem, router portatili GSM, ecc.).

Ogni utente deve prestare la massima attenzione ai supporti di provenienza esterna di cui ne venisse in possesso, avvertendo immediatamente il personale del Servizio IT.

Ogni file personale salvato sul PC si considera di proprietà dell'Azienda, in quanto collegato alla rete aziendale.

I files e i documenti (dati) generati nel corso dell'attività lavorativa e di natura permanente, ovvero di valore rilevante per le attività aziendali, non devono essere conservati stabilmente sul PC dell'utente ma salvati nella propria cartella del server, protetta da sistemi di backup per garantire la continuità delle attività aziendali anche in caso di grave guasto al PC. Il Servizio IT deve essere interpellato per definire la periodicità e la destinazione del riversamento in base alle caratteristiche dei dati da proteggere.

PC Laptop (portatili)

L'utente è responsabile del PC portatile assegnatogli dall'Azienda. Esso deve essere custodito con la massima diligenza durante gli spostamenti.

Ai PC portatili si applicano tutte le regole di utilizzo dei PC fissi.

Inoltre, a maggior ragione durante il loro utilizzo in mobilità, il portatile non deve mai essere lasciato incustodito e deve essere adeguatamente preservato nei luoghi e con i mezzi più idonei per la sua ottimale protezione.



Nel disco fisso del portatile devono essere immagazzinate esclusivamente le informazioni strettamente necessarie all'attività inerente al proprio ruolo, al fine di limitare la perdita di informazioni aziendali in caso di danno, smarrimento o furto.

In caso di smarrimento o furto del portatile, l'utente ha l'obbligo d'informare tempestivamente il proprio Responsabile di Funzione e il Responsabile del Servizio IT (supporto@mondialpol.it), nonché di denunciare immediatamente l'accaduto alle Forze dell'Ordine, fornendo alla Società, la copia dell'atto di denuncia.

In situazioni potenzialmente a rischio, è necessario che il Dipendente attivi cautele e presidi più restrittivi rispetto alla custodia del PC fisso.

Tali situazioni sono:

- trasporto in automobile: è severamente vietato lasciare incustodito il portatile all'interno dell'automobile, anche per brevi periodi (la violazione di una vettura e conseguente asportazione di oggetti contenuti, avviene in pochi secondi);
- pernottamenti in albergo: è obbligatorio prestare la massima diligenza e prudenza per il portatile durante le permanenze in albergo. I portatili sono spesso dotati di presa universale per il fissaggio con appositi cavi con lucchetto. In questi casi si può lasciare il portatile in camera opportunamente ancorato (evitare ad es. la gamba di un tavolo), ovvero lasciato in custodia presso la reception, ma avendo l'accortezza di apporre un'etichetta di sicurezza (monouso) firmata dall'utente. In caso di violazione dell'etichetta il Dipendente dovrà effettuare una segnalazione all'Azienda e al personale preposto al Servizio IT, comunicando i dati relativi al portatile, nonché le circostanze dell'accaduto.

L'eventuale uso promiscuo (anche per fini personali) del PC portatile aziendale, è possibile soltanto in presenza di preventiva autorizzazione scritta e/o a seconda degli accordi contrattuali definiti col Dipendente e in conformità alle istruzioni al riguardo impartite dal personale del Servizio IT.

L'eventuale uso promiscuo (anche per fini aziendali) del PC portatile personale, è possibile soltanto in presenza di preventiva autorizzazione scritta e/o a seconda degli accordi contrattuali definiti col Dipendente e in conformità alle istruzioni al riguardo impartite dal personale del Servizio IT.

L'autorizzazione all'utilizzo di software acquistati con licenza d'uso concessa a Vedetta 2 Mondialpol su dispositivi personali, anche se utilizzati per conto dell'Azienda, compresa anche la sola connessione alla rete informatica aziendale (MPLS/VPN), implica tacita autorizzazione dell'utente a procedere allo screening degli applicativi ivi installati per tramite del personale dell'Ufficio IT.

In caso di cessazione del rapporto con l'Azienda, il PC portatile completo degli accessori deve essere riconsegnato al personale del servizio IT (supporto@mondialpol.it).

Qualora il Dipendente abbia necessità di salvare e conservare una limitata quantità di dati e informazioni personali non inerenti l'attività lavorativa, deve provvedere a salvare tali dati in un'apposita cartella creata dall'utente e denominata "Privatedocs - nome utente" (es. Privatedocs - Mario Rossi).

Telefoni cellulari - smartphones

Il telefono cellulare aziendale può essere utilizzato solo per ragioni di servizio ed è obbligo di ogni assegnatario farne un uso appropriato ed averne una diligente conservazione.

Fermo restando quanto più avanti disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS o MMS ivi compresi messaggi che utilizzano la rete dati (Whatsapp, Telegram, ecc.), di natura personale o comunque non pertinenti rispetto allo



svolgimento dell'attività lavorativa, viene consentita solo nel caso di comprovata necessità e urgenza o in assenza di alternative praticabili.

L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale, è possibile soltanto in presenza di preventiva autorizzazione scritta e/o a seconda degli accordi contrattuali definiti col Dipendente e in conformità alle istruzioni al riguardo impartite dal personale del Servizio IT.

L'eventuale uso promiscuo (anche per fini aziendali) del telefono cellulare personale, è possibile soltanto in presenza di preventiva autorizzazione scritta e/o a seconda degli accordi contrattuali definiti col Dipendente e in conformità alle istruzioni al riguardo impartite dal personale del Servizio IT.

L'autorizzazione all'utilizzo di software acquistati con licenza d'uso concessa a Vedetta 2 Mondialpol su dispositivi personali, anche se utilizzati per conto dell'Azienda, compresa anche la sola connessione alla rete informatica aziendale (MPLS/VPN), implica tacita autorizzazione dell'utente a procedere allo screening degli applicativi ivi installati per tramite del personale dell'Ufficio IT.

L'apparecchio affidato al Dipendente non può essere concesso in uso a colleghi o terzi.

L'utilizzatore prenderà in consegna il telefono cellulare previa sottoscrizione di dichiarazione di conoscenza delle disposizioni del presente Regolamento.

In caso di malfunzionamento del cellulare e/o della relativa scheda SIM e/o dei relativi accessori, l'utilizzatore dovrà consegnare l'apparecchiatura completa al referente del Servizio Telefonia Mobile Aziendale che provvederà alle verifiche di competenza e all'eventuale sostituzione.

In caso di smarrimento o di furto del cellulare, l'utilizzatore è tenuto a sporgere immediata denuncia alle autorità competenti, preferibilmente della località ove si è verificato l'evento, e a darne tempestiva comunicazione all'Azienda, fornendo copia della denuncia, e al Referente della Telefonia Mobile.

Nella comunicazione dovrà essere indicato in particolare il numero telefonico della SIM abbinata al cellulare al fine di consentire l'operazione di blocco immediato (SIM e cellulare).

In caso di ripetuti smarrimenti, furti, guasti o quant'altro, l'assegnazione del cellulare potrà essere revocata.

L'Azienda si riserva la facoltà di revocare o sospendere l'assegnazione del cellulare e chiederne la restituzione, per mancato utilizzo, per politica aziendale e comunque a suo insindacabile giudizio, con obbligo per l'utilizzatore di immediata riconsegna all'Azienda e/o al referente della Telefonia Mobile Aziendale (antonino.vitale@mondialpol.it).

In caso di cessazione del rapporto con l'Azienda, il telefono completo degli accessori e relativa SIM devono essere riconsegnati al referente della Telefonia Mobile Aziendale (antonino.vitale@mondialpol.it).

Qualora il Dipendente abbia necessità di salvare e conservare una limitata quantità di dati e informazioni personali non inerenti l'attività lavorativa, deve provvedere a salvare tali dati in un'apposita cartella creata dall'utente e denominata "Privatedocs - nome utente" (es. Privatedocs - Mario Rossi).

L'utente resta responsabile del dispositivo assegnato e deve custodirlo sempre con la diligenza del buon padre di famiglia; va sempre adottata ogni cautela per evitare danni o sottrazioni. Al fine di evitare qualsivoglia accesso e utilizzo non autorizzato o illecito, è fatto obbligo che ciascun dispositivo venga protetto, a cura dell'utente, con una password che dovrà soddisfare i criteri dettati al paragrafo "Gestione della UserID e Password".



In particolare è necessario non separarsi mai dal dispositivo, e lo stesso deve essere messo in sicurezza attivando il blocco automatico che deve avvenire entro un brevissimo lasso di tempo dall'inutilizzo, ovvero manualmente.

Uscendo da un locale pubblico o da un taxi, si deve sempre verificare di avere il cellulare con sé.

Al momento della restituzione, l'utente ha l'obbligo di cancellare qualsiasi informazione contenuta, ivi compresi, a mero titolo esemplificativo e non esaustivo, contatti in rubrica, impegni in agenda, messaggi, fotografie, video, eventuali App non preinstallate che raccolgono dati, e quant'altro, mediante il reset totale dell'apparato per riportarlo alla condizione di "primo utilizzo".

Ogni dispositivo deve essere impostato con un blocco automatico che si attivi dopo un brevissimo lasso di tempo dal suo inutilizzo, oppure attivato manualmente. Tale blocco deve consistere in una password creata secondo le regole dettate al paragrafo "Gestione della UserID e Password". La password deve essere nota solo all'utente, e non deve essere mai comunicata a colleghi o terzi (conoscenti, amici, parenti, ecc.).

In caso di manutenzione ad opera del personale del Servizio IT, dovrà essere disattivata la funzione dello sblocco con password.

Ogni dispositivo è configurato con sistemi di filtraggio della navigazione per impedire l'accesso a contenuti pericolosi o inappropriati; è vietato modificare le impostazioni relative all'APN o qualsiasi altra impostazione al fine di aggirare il sistema di filtraggio o blocco dei contenuti.

Palmari e tablet

Tutti i dispositivi elettronici in dotazione al personale dell'Azienda devono considerarsi strumenti di lavoro; ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative. Non sono quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative.

Per i palmari e i tablet valgono le stesse prescrizioni dettate in tema di telefoni cellulari aziendali. In particolare è necessario non lasciare mai incustodito il dispositivo, ed è fatto obbligo di conservarlo e utilizzarlo prestando la massima cautela e diligenza. Il Dipendente a cui è dato in dotazione un dispositivo elettronico aziendale, ne è considerato diretto responsabile, anche ai fini del suo funzionamento e della sua integrità.

Ogni dispositivo deve essere impostato con un blocco automatico che si attivi dopo un brevissimo lasso di tempo dal suo inutilizzo, oppure attivato manualmente. Tale blocco deve consistere in una password creata secondo le regole dettate al paragrafo "Gestione della UserID e Password". La password deve essere nota solo all'utente, e non deve essere mai comunicata a colleghi o terzi, salvo i casi di manutenzione ad opera del personale del Servizio IT.

Ogni dispositivo è configurato con sistemi di filtraggio della navigazione per impedire l'accesso a contenuti pericolosi o inappropriati, è vietato modificare le impostazioni relative all'APN o qualsiasi altra impostazione al fine di aggirare il sistema di filtraggio o blocco dei contenuti.

L'eventuale uso promiscuo (anche per fini personali) del palmare o tablet aziendale, è possibile soltanto in presenza di preventiva autorizzazione scritta e/o a seconda degli accordi contrattuali definiti col Dipendente e in conformità alle istruzioni al riguardo impartite dal personale del Servizio IT.

L'eventuale uso promiscuo (anche per fini aziendali) del palmare o tablet personale, è possibile soltanto in presenza di preventiva autorizzazione scritta e/o a seconda degli accordi contrattuali definiti col Dipendente e in conformità alle istruzioni al riguardo impartite dal personale del Servizio IT.



L'autorizzazione all'utilizzo di software acquistati con licenza d'uso concessa a Vedetta 2 Mondialpol su dispositivi personali, anche se utilizzati per conto dell'Azienda, compresa anche la sola connessione alla rete informatica aziendale (MPLS/VPN), implica tacita autorizzazione dell'utente a procedere allo screening degli applicativi ivi installati per tramite del personale dell'Ufficio IT.

In caso di cessazione del rapporto con l'Azienda, il palmare e/o tablet completo degli accessori ed eventuale relativa SIM, devono essere riconsegnati al referente della Telefonia Mobile Aziendale (antonino.vitale@mondialpol.it).

Qualora il Dipendente abbia necessità di salvare e conservare una limitata quantità di dati e informazioni personali non inerenti l'attività lavorativa, deve provvedere a salvare tali dati in un'apposita cartella creata dall'utente e denominata "Privatedocs - nome utente" (es. Privatedocs - Mario Rossi).

Utilizzo di altre attrezzature elettroniche aziendali

E' precluso l'utilizzo per fini personali di fax, sia per l'invio che per la ricezione, di fotocopiatrici e di stampanti, salva diversa esplicita autorizzazione da parte del Responsabile gerarchico.

Dispositivi e supporti di memoria rimovibile e/o portatile

Mondialpol mette a disposizione ampi spazi di archiviazione (NAS, server Zucchetti, server di posta ecc.) con elevati livelli di protezione in caso di eventi che possano precludere l'utilizzo temporaneo dei dati. Su tali sistemi devono essere archiviati i relativi dati. Pertanto, per evidenti motivi di sicurezza, è precluso l'utilizzo di dispositivi di memoria rimovibili (dischi fissi rimovibili, CD/DVD riscrivibili, chiavette USB ecc.).

Solo i Responsabili di Centrale Operativa (limitatamente a quanto di loro spettanza) e gli addetti del Servizio IT sono autorizzati alla creazione di supporti rimovibili con l'esportazione di files che fossero richiesti ad esempio dalle FF.OO. o casi assimilabili.

GESTIONE DELLA USERID E PASSWORD

Le credenziali di autenticazione consistono in una UserID e una password che dovranno essere custodite dall'utente con la massima accortezza.

Le credenziali di autenticazione per l'accesso al personal computer o a un sistema, sono strettamente personali e non vanno comunicate o condivise con chicchessia per alcun motivo.

Le credenziali di autenticazione per l'accesso a un dispositivo o a un sistema, vengono assegnate all'Utente dall'Amministratore di Rete o dall'Amministratore di Sistema su richiesta del Responsabile di Funzione.

Eventuali variazioni, modifiche o richieste di disattivazione delle credenziali di accesso devono essere richieste dal Responsabile di Funzione tramite apertura di ticket aziendale (supporto@mondialpol.it).

Le credenziali di autenticazione privilegiate o di amministrazione sono fornite agli utenti delegati a operare nel ruolo di Amministratori di sistema su autorizzazione del CIO.

Le procedure di sicurezza e gestione agli accessi dei software in uso in Mondialpol, devono essere progettate in modo da implementare in modo non eludibile dall'utente le politiche di sicurezza password descritte in questo documento.

Eventuali nuovi software che siano adottati in Azienda o in caso di aggiornamento di software esistenti, devono preferibilmente implementare un sistema di SSO in modo da limitare il numero di credenziali assegnate all'utente.



In Mondialpol non è consentita l'attivazione della password di accensione (c.d. bios), senza preventiva autorizzazione da parte del Servizio IT.

Caratteristiche della password

La password deve essere composta da almeno dieci caratteri e deve soddisfare almeno tre delle seguenti quattro caratteristiche:

- contenere una lettera minuscola
- contenere una lettera maiuscola
- contenere un numero
- contenere un carattere speciale

La password non deve contenere riferimenti agevolmente riconducibili all'utente (nome o cognome o parti di essi, date, ricorrenze, ecc.) e deve essere modificata da quest'ultimo al primo accesso e, successivamente, almeno ogni sei mesi, e ogni qualvolta pervenga la richiesta automatica del sistema.

È necessario adottare le necessarie cautele per assicurare la segretezza della password e la diligente custodia degli eventuali dispositivi in uso.

Trascorsi sei mesi di inutilizzo delle credenziali di autenticazione, queste potranno essere disattivate automaticamente o manualmente a cura dell'Amministratore di Sistema.

Qualora nell'arco temporale di 10 minuti si verifichino consecutivamente più di cinque tentativi di accesso con password errata (credenziali utente di dominio), l'account sarà sospeso temporaneamente per un periodo non inferiore a 30 minuti.

Qualora l'utente cambi mansione o ufficio o non sia più in possesso delle autorizzazioni necessarie, l'account (credenziali) viene disattivato.

Al fine di una sicura gestione delle credenziali, e allo scopo di preservare la rete e le risorse informatiche aziendali da accessi non autorizzati, è necessario che l'utente/Dipendente:

- non permetta ad altri di operare con le proprie credenziali nemmeno se si è presenti durante l'attività; concedere ad altri le proprie credenziali di accesso a un sistema, fa ricadere su di sé la responsabilità delle operazioni che vengono eseguite;
- non trascriva le credenziali su foglietti, post-it ovvero sul dispositivo medesimo, né le memorizzi nel PC;
- non le comunichi mai per telefono; in caso di sospetta compromissione delle credenziali, si deve provvedere immediatamente al cambio delle medesime, ovvero ci si deve rivolgere immediatamente all'Amministratore di Sistema per richiederne il reset e ottenerne di nuove;
- nel caso un utente venga a conoscenza delle credenziali di un altro utente, è tenuto a informarlo immediatamente; questi dovrà provvedere al cambio immediato, e dovrà avvisare la funzione Audit/OdV (audit@mondialpol.it, odv.vedetta2mondialpol@mondialpol.it) specificandone le circostanze per le necessarie valutazioni dell'accaduto e porvi gli eventuali correttivi.

Scelta, custodia, modifica e utilizzo della password devono rispettare le prescrizioni contenute nella presente Policy. Si ricorda, a tale riguardo, che:

- al primo accesso ad un sistema e/o ad una banca dati, l'utente è tenuto a cambiare la password assegnatagli dall'Amministratore di Sistema, anche se l'operazione non viene richiesta in automatico dal sistema stesso;
- in un sistema, la UserID è univoca ed è associata a uno specifico utente;



- l'accesso ai sistemi informativi deve poter essere tracciato, pertanto non è consentito accedere a sistemi informativi utilizzando credenziali di altri utenti.

RETE TELEMATICA INTERNA AZIENDALE (MPLS)

L'MPLS è l'insieme delle tecnologie mediante le quali si realizza la connettività interna tra i vari componenti del sistema informatico aziendale e tra le varie Sedi/Filiali. Per semplificare, la rete aziendale di Vedetta 2 Mondialpol è una MPLS. Le impostazioni dei PC sono predisposte dallo Staff IT sulla base di criteri e profili decisi dalla Direzione, in funzione della qualifica del Dipendente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilita dalla Direzione stessa. È preclusa al Dipendente la modifica di tali impostazioni.

Tutti i software installati sul sistema operativo, e in particolare i software necessari per la protezione dello stesso o della rete internet (es. antivirus o firewall virtuali) non possono essere disinstallati o in nessun modo manomessi dai Dipendenti, salvo quando questo sia richiesto dall'Amministratore di Sistema per compiere attività di manutenzione o aggiornamento.

La rete aziendale è dotata di sistemi di filtraggio della navigazione per impedire l'accesso a contenuti pericolosi o inappropriati; è vietato modificare le impostazioni del PC o installare qualsiasi software al fine di aggirare o eludere il sistema di filtraggio o blocco dei contenuti.

Le password d'accesso alla MPLS e ai programmi di rete sono strettamente riservate e personali, e vanno comunicate e gestite secondo le procedure in precedenza descritte.

Alla luce di ciò, salvo previa autorizzazione scritta di CIO/CISO o IT Manager o Amministratore di Rete, è fatto esplicito divieto di:

- utilizzare la rete aziendale per fini non espressamente previsti e/o autorizzati;
- connettere in rete locale apparecchiature elettroniche (PC, stampanti, switch, router, modem, ecc.).

Riscontrando la presenza di apparecchiature elettroniche e/o software non autorizzato, questi verranno rimossi.

Nella gestione delle apparecchiature informatiche aziendali, il Servizio IT potrà acquisire informazioni generate dalle funzionalità insite negli stessi sistemi quali, ad esempio, le informazioni sugli orari di accensione e spegnimento dei personal computer, rilevati automaticamente tramite il sistema di autenticazione alla rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate per tutti i fini connessi al rapporto di lavoro con espressa esclusione di qualsiasi forma di monitoraggio sistematico e costante nei confronti degli utenti.

INTERNET - ACCESSO e NAVIGAZIONE

Il PC assegnato al singolo utente e abilitato alla navigazione in Internet, costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

Mondialpol adotta modalità finalizzate a bloccare l'accesso a siti internet ritenuti non consoni allo svolgimento dell'attività lavorativa e/o comunque non affidabili.

Mondialpol definisce la modalità di accesso ad Internet mediante l'utilizzo di una "whitelist". I siti internet non presenti nella whitelist sono automaticamente bloccati. E' vietato installare software o modificare le impostazioni del dispositivo in dotazione al fine di aggirare o eludere il sistema di filtraggio o blocco dei contenuti.



Per ottenere lo sblocco di uno specifico sito internet di pubblico interesse, l'utente deve aprire un ticket sul sistema di supporto informatico (supporto@mondialpol.it). Nel ticket deve essere riportato l'esatto link del sito richiesto.

È preclusa a ogni utente la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

È precluso a ogni utente l'utilizzo delle c.d. "saponette" o qualsivoglia dispositivo WiFi portatile dotato di SIM, per la navigazione in Internet.

In questo senso, a titolo puramente esemplificativo, all'utente è preclusa la navigazione in internet per i seguenti scopi:

- l'upload o il download di dati e/o software anche gratuiti (freeware) e shareware;
- effettuare il download di documenti e/o dati, se non strettamente attinenti all'attività lavorativa e salvo previa verifica dell'attendibilità dei siti in questione e approvazione del Servizio IT;
- effettuare ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti online e simili per motivi personali, fatti salvi i casi direttamente autorizzati dalla Direzione Generale;
- registrarsi a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- partecipare a Forum non professionali, utilizzare account email aziendali per registrarsi su siti internet, utilizzare servizi di chat e messaggistica istantanea (esclusi gli strumenti autorizzati) o bacheche elettroniche e registrarsi anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal proprio Responsabile diretto;
- accedere ad account personali di servizi webmail di posta elettronica.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, Mondialpol adotta anche una "black list" automaticamente aggiornata.

Eventuali controlli sulla navigazione effettuati dal Responsabile Protezione Dati tramite il Servizio IT, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione.

Il controllo sui file di log non è continuativo, e i files stessi vengono conservati non oltre il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Azienda.

L'utilizzo di tutte le reti WiFi presenti in Azienda è limitato agli utenti autorizzati. Per accedere alle reti WiFi dell'Azienda occorrono specifiche credenziali che verranno assegnate dal Servizio IT.

Accesso alla rete aziendale tramite VPN

L'accesso da remoto alla rete aziendale, avviene tramite il rilascio di una VPN autenticata. La VPN autenticata viene rilasciata, su richiesta motivata dell'utente, dall'Amministratore di Rete. La VPN autenticata identifica l'utente che accede da remoto alla rete aziendale.

L'accesso alla rete aziendale mediante VPN autenticata, è possibile solo utilizzando i dispositivi previsti. Vengono effettuati controlli automatici che impediscono l'accesso mediante utilizzo di dispositivi non abilitati.



AUDITING AZIENDALE e ORGANISMO DI VIGILANZA

Audit aziendale

La funzione di Audit aziendale ha facoltà di accedere alla rete aziendale e ai dispositivi ad essa connessi secondo sue insindacabili scelte e ai soli esclusivi fini della verifica del rispetto del presente Regolamento e della normativa in tema di protezione dei dati personali, anche tramite l'Amministratore di Rete e/o l'Amministratore di Sistema.

La funzione Audit informa preventivamente l'RPD sulle attività che intende intraprendere, specificandone anche un limite temporale.

Organismo di Vigilanza

La stessa facoltà, con le medesime modalità, è riconosciuta all'Organismo di Vigilanza nominato ai sensi del D.lgs. 231/2001, informando il Responsabile Protezione Dati (RPD). L'Organismo di Vigilanza informa preventivamente l'RPD sulle attività che intende intraprendere, specificandone anche un limite temporale.

POSTA ELETTRONICA ORDINARIA AZIENDALE (PEO)

Generalità

Mondialpol fornisce il servizio di PEO ai Dipendenti che ne necessitano per lo svolgimento della propria attività lavorativa.

Il servizio implica la fornitura di un account email con nome utente e password, avente dominio di proprietà di Mondialpol, quali ad esempio: mondialpol.it, mondialpol.com, mondialpol.email e altri.

Account di posta elettronica

Per ottenere in uso un account aziendale di posta elettronica, è necessario che il Responsabile di Funzione compili l'apposito modulo online, disponibile sulla Extranet (Callisto).

All'utente verranno fornite le credenziali di accesso e le principali informazioni per la configurazione dell'account sul proprio client di posta. La password deve assolutamente essere personalizzata al primo accesso, anche se non richiesto dal sistema.

Per evidenti motivi di sicurezza, praticità e funzionalità, l'account dovrà essere configurato sul proprio client di posta, esclusivamente col protocollo IMAP.

L'utente è responsabile del corretto utilizzo dell'account di posta assegnato.

L'account assegnato nonché tutto il traffico derivante da tale account, sia in entrata che in uscita, è classificato come documentazione aziendale e, pertanto, di proprietà di Mondialpol.

È precluso l'utilizzo della posta elettronica aziendale per motivi non inerenti all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- invio/ricezione di allegati multimediali (immagini, video, audio) non legati all'attività lavorativa;
- invio/ricezione di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list o registrazione a siti internet non inerenti all'attività lavorativa;
- far circolare le c.d. "catene di sant'antonio". In presenza di allegati in tali messaggi, non si dovrà compiere alcuna azione.



Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Azienda, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservato" o analoga dicitura, deve essere portata a conoscenza del proprio Responsabile.

Solo il personale abilitato a impegnare la Società può utilizzare l'email per fini di negoziazione contrattuale. Non esiste attualmente un sistema di posta elettronica in grado di distinguere automaticamente gli utenti dotati di potere di rappresentanza dell'Azienda da chi non li ha.

Resta esclusa qualsiasi responsabilità dell'Azienda per la conclusione, stipulazione o adesione a qualsiasi proposta/modifica/negoziazione di contratto, ed è onere del terzo sincerarsi del potere di rappresentanza dell'utente con cui scambia email.

È compito dei Responsabili di Funzione o comunque dei superiori gerarchici, comunicare immediatamente la cessazione di un utente di posta elettronica all'Amministratore di Sistema e richiederne la disabilitazione ed eventualmente l'attivazione dei servizi di risposta automatica e, se pertinente, l'inoltro. Tali servizi avranno comunque una durata limitata nel tempo (max. 60 gg.).

Cambio della password della posta elettronica

Per motivi non dipendenti da Mondialpol, il sistema di posta elettronica non obbliga l'utente a cambiare la password al primo login, quindi è fatto obbligo all'utente, di impostare immediatamente una nuova password.

La password della posta elettronica scade dopo un periodo preimpostato. All'approssimarsi della data di scadenza, il sistema invia svariate email che invitano l'utente a cambiare la password.

L'utente non deve ignorare i messaggi automatici che ricordano il termine della scadenza della password.

Alla scadenza del termine di validità della password senza che questa sia stata cambiata, l'account di posta verrà automaticamente bloccato e non sarà più accessibile.

È possibile richiedere il reset della password tramite il sistema di ticket (supporto@mondialpol.it).

Le credenziali di accesso vengono di norma inviate mediante una notifica automatica sul proprio account email personale nel momento in cui l'account aziendale è attivo e disponibile.

Allegati di posta

L'utente è tenuto a porre la massima attenzione nell'aprire allegati di qualsiasi natura, se non si ha l'assoluta certezza della provenienza (identità del mittente). Soprattutto in presenza di allegati con estensione .exe o .zip (files compressi), l'utente deve informare tempestivamente il Servizio IT ovvero l'Amministratore di Rete, senza compiere alcuna altra azione. Di norma gli allegati con estensione .exe e .zip vengono rimossi dal sistema.

Nel caso si abbia il ragionevole dubbio di aver aperto accidentalmente un qualsiasi allegato che possa compromettere la sicurezza della rete aziendale, l'utente deve immediatamente scollegare il PC dalla rete elettrica e informatica, e avvisare tempestivamente il Servizio IT.

Spazio di archiviazione della casella di posta - backup

Lo spazio di default assegnato ad ogni account di posta elettronica è di 3GB.

L'utente è tenuto a eliminare tutta la corrispondenza inutile al fine di evitare, per quanto possibile, il raggiungimento della quota assegnata.



All'avvicinarsi del raggiungimento della quota di archiviazione, l'utente riceve una sequenza di messaggi automatici che avvertono dell'approssimarsi di tale limite. È possibile richiedere all'Amministratore di Sistema, spazio aggiuntivo di archiviazione (supporto@mondialpol.it). Di norma, al raggiungimento o superamento della quota di 15 GB di spazio di archiviazione, può essere assegnato un account su Mail Store (v. par. successivo).

È preclusa all'utente la facoltà di creare archivi .pst o quant'altro, sia al fine di alleggerire la casella di posta che al fine di effettuare backup.

Non è consentito l'utilizzo del Cestino quale archivio dei messaggi di posta per una successiva consultazione. Il Cestino della posta elettronica si svuota automaticamente.

Ulteriori informazioni sono disponibili sulla extranet (Callisto).

Mail Store

Agli utenti che hanno straordinarie necessità di archiviazione, viene assegnato un account sul server Mail Store.

A seguito dell'assegnazione dell'account su Mail Store, solitamente vengono lasciati gli ultimi sei mesi di corrispondenza online, mentre il pregresso viene trasferito su Mail Store.

Mail Store dà la possibilità di consultare e cercare la posta ivi archiviata, come in un normale client di posta. È inoltre possibile l'eventuale ripristino di singoli messaggi nel server di posta principale.

Mail Store non funge da backup, ma solo quale spazio aggiuntivo di archiviazione.

Ulteriori informazioni sono disponibili sulla extranet (Callisto).

Messaggio per assenza

Resta a cura dell'utente, in caso di periodi di assenza programmata, impostare la risposta automatica indicando il nominativo e il relativo indirizzo di posta a cui ci si dovrà rivolgere in caso di urgenza. Tale impostazione dovrà essere disattivata al rientro dal periodo di assenza.

In caso di assenza improvvisa o non programmata, la risposta automatica potrà essere attivata dall'Amministratore di Sistema qualora ne sia portato a conoscenza.

Sospensione/disattivazione di account di posta elettronica

L'Azienda, a proprio insindacabile giudizio, ha facoltà di attivare o eliminare utenze di posta elettronica, in base alla valutazione della necessità di utilizzo per lo svolgimento dell'attività lavorativa.

La casella di posta elettronica viene disattivata al momento della cessazione del rapporto contrattuale. L'Azienda si riserva, tuttavia, di valutare a proprio esclusivo ed insindacabile giudizio la necessità di mantenere attiva, ma non più raggiungibile dall'utente, la casella per un congruo periodo di tempo per consentire il funzionamento del servizio automatico di risposta automatica e/o di inoltrare, al fine di garantire la funzionalità e continuità aziendale.

È compito dei Responsabili di Funzione o comunque dei superiori gerarchici, comunicare immediatamente la cessazione di un utente di posta elettronica aziendale all'Amministratore di Sistema e richiederne la disabilitazione ed eventualmente l'attivazione dei servizi di risposta automatica e, se pertinente, l'inoltrare. Tali servizi avranno comunque una durata limitata nel tempo (max. 60 gg.).



Nel caso in cui l'utente abbia anche la gestione di uno o più account di Posta Elettronica Certificata (PEC), questi dovrà attenersi a quanto previsto nel presente Regolamento.

Posta Elettronica Certificata (PEC)

L'Amministratore di Sistema delle PEC è il fornitore del servizio. L'account PEC viene richiesto dal Responsabile di Funzione mediante la compilazione di apposito modulo reperibile sulla Extranet (Callisto).

Data la peculiarità delle caratteristiche della corrispondenza che intercorre a mezzo PEC, la gestione dell'account PEC avviene tramite l'apposita piattaforma Pec Organizer.

Le funzionalità di Pec Organizer consentono che il medesimo account di PEC possa essere gestito e condiviso tra più utenti.

L'efficacia di una comunicazione di PEC si esaurisce nel momento in cui la corrispondenza intercorra con altro indirizzo PEC.

Ulteriori informazioni sono disponibili sulla extranet (Callisto).

SPAM

È espressamente vietato l'utilizzo della posta elettronica nel momento in cui si traduce in un danno o semplicemente un disturbo a terzi; ad esempio l'invio indiscriminato di messaggi di posta elettronica indirizzata ad un medesimo soggetto, l'invio massivo di materiale pubblicitario e/o commerciale non richiesto, l'utilizzo di mailing list di soggetti terzi che non abbiano espressamente dato il consenso, innescare o rispondere alle c.d. "catene di S. Antonio", ecc.

Invio massivo di messaggi di posta

Si raccomanda di evitare l'invio di comunicazioni a un elevato numero di destinatari onde evitare che il sistema di posta sia bloccato e messo in black list.

L'invio massivo di messaggi di posta deve possedere determinate caratteristiche

Qualora sia necessario dover procedere con l'invio massivo di un messaggio di posta elettronica, es. una circolare a Clienti o Fornitori, si deve fare richiesta all'Amministratore di Sistema (supporto@mondialpol.it).

Backup della posta elettronica

Il backup della posta elettronica aziendale viene effettuato su apposito server, e ha una durata di 10 giorni. Oltre questo termine non sarà più possibile recuperare i dati.

Nel caso si debba ricorrere, per motivi accidentali o involontari, a ripristinare un backup, ci si deve rivolgere immediatamente all'Amministratore di Sistema.

Non è consentito il backup della posta elettronica aziendale con metodologie diverse da quella qui descritta. Non è consentito il backup della posta elettronica su server diversi da quello appositamente predisposto.

Amministratore di Sistema della posta elettronica

L'Amministratore di Sistema della posta elettronica è la persona lecitamente autorizzata a trattarne i dati nello svolgimento della sua mansione, e nel rispetto della privacy dell'Utente. Qualora, durante una verifica o una manutenzione, venga incidentalmente a conoscenza di un illecito, atto a danneggiare l'Azienda, potrà porre in atto tutte le misure tecnologiche idonee a far sì che tale illecito non sia perpetrato ovvero a mantenerne le prove qualora l'illecito sia già stato consumato.



VIRUS INFORMATICI E ANTIVIRUS

I virus informatici sono in costante sviluppo ed evoluzione, e gli antivirus sono e resteranno sempre un passo indietro rispetto ad essi. È per questo motivo che è necessario che gli antivirus siano sempre costantemente aggiornati.

I PC fissi e portatili, i tablet, i palmari e gli smartphones in dotazione agli utenti, pur protetti contro gli attacchi da virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus o malware non conosciuti. Per ridurre le probabilità del verificarsi di tali attacchi, è necessario che vengano osservate le seguenti regole:

- verificare che il programma antivirus sia attivo;
- non aprire files sospetti o di dubbia provenienza;
- diffidare da messaggi scritti con una sintassi errata;
- non scaricare e/o installare applicazioni e software. Tale attività è di esclusiva competenza del Servizio IT;
- porre la necessaria attenzione sulle eventuali segnalazioni di anomalie inviate dal PC durante l'attività, e segnalarle al supporto IT;
- non modificare le configurazioni impostate sul proprio PC, le configurazioni di rete e dell'antivirus;
- prestare attenzione ai bollettini aventi per oggetto AVVISO DI SICUREZZA.

In caso di malfunzionamento o rallentamento delle prestazioni del PC, che può far sospettare la presenza di un virus, l'utente deve:

- interrompere ogni attività sul PC;
- disconnettere il PC dal cavo di rete o dalla rete Wi-Fi e dall'alimentazione elettrica;
- se possibile, scattare con lo smartphone una fotografia di quanto rappresentato sullo schermo, eventualmente richiedendo l'aiuto ai colleghi;
- contattare immediatamente il Servizio IT;
- disconnettere il PC dalla rete informatica o spegnerlo del tutto se è evidente la presenza di virus, in attesa di ulteriori indicazioni dal Servizio IT.

Ogni supporto di memoria di provenienza esterna all'Azienda dovrà essere verificato dallo Staff IT mediante il programma antivirus prima del suo utilizzo.

SALVATAGGIO DEI DATI - BACKUP

Per motivi di sicurezza, tutti i documenti rilevanti ai fini dell'attività lavorativa devono essere salvati su server aziendale o NAS, per protezione da eventuali guasti della postazione personale.

A tale riguardo, l'utente può richiedere al Servizio IT che sia resa disponibile sul server una cartella personale o una cartella condivisa con il gruppo di lavoro cui fa riferimento l'utente stesso.

Non è consentito per alcun motivo effettuare copie di dati aziendali su dispositivi personali (chiavette USB, dischi esterni, CD, DVD, ecc.) anche se tali dispositivi non sono portati fuori dall'azienda, a prescindere che sussista o meno l'ipotesi di divulgazione di dati aziendali.

Come già detto, non è consentito il salvataggio/backup del proprio account di posta elettronica (es. archivi .pst) su dispositivi rimovibili, tantomeno la trasmissione di dati aziendali ad una casella di posta elettronica personale per fini di archiviazione.



VERIFICHE DA PARTE DELL'AZIENDA E PRINCIPIO DI PERTINENZA E NON ECCEDENZA

Mondialpol si riserva la facoltà di verificare, per finalità di sicurezza e tutela del proprio patrimonio, l'esistenza di un comportamento illecito nell'uso degli strumenti elettronici, l'accesso a Internet e sull'uso della posta elettronica.

Le verifiche si effettueranno nel rispetto della libertà, della segretezza delle comunicazioni e delle garanzie previste dallo Statuto dei lavoratori e dal Codice Privacy, e verranno effettuate da personale lecitamente autorizzato.

In particolare sarà possibile verificare gli accessi a internet e i tempi di connessione, senza indagare sui siti oggetto di accesso, in ottemperanza a quanto previsto dal GDPR. A seguito delle verifiche potranno essere raccolti dati personali che saranno trattati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza della finalità di tutela della sicurezza e del patrimonio.

Eventuali informazioni di natura sensibile - compreso il contenuto di email trasmesse o ricevute dalle caselle di posta aziendale o l'elenco di siti oggetto di accesso - potranno essere trattate dalle figure preposte (Organismo di Vigilanza, Responsabile Protezione Dati, Internal Audit) a norma di Legge.

Qualora, durante una verifica, l'Azienda venga incidentalmente a conoscenza di un illecito commesso dal Dipendente, l'Azienda potrà adottare tutti i provvedimenti disciplinari e/o legali da cui tale illecito potrebbero scaturire.

ASPETTI DI PRIVACY PER IL DIPENDENTE

I files caricati sui PC fissi e portatili e sugli altri dispositivi aziendali, nonché le email aziendali, sono di proprietà dell'azienda.

E' fatto divieto ai Dipendenti di:

- effettuare copie non autorizzate su supporti non aziendali o trasmissioni non autorizzate di dati inerenti l'attività lavorativa;
- fare copie fotostatiche o di qualsiasi altra natura, non autorizzate, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati inerenti all'attività lavorativa;
- sottrarre, cancellare, modificare, alterare, distruggere senza l'autorizzazione, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati inerenti all'attività lavorativa;
- consegnare a persone non autorizzate, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati inerenti all'attività lavorativa, sia in formato elettronico che cartaceo.

La cattiva gestione o la sottrazione o distrazione di documenti cartacei, esula dal regolamento di utilizzo degli strumenti informatici.

Nel caso in cui l'Azienda debba accedere all'archivio informatico presente su un qualunque dispositivo aziendale assegnato all'utente per finalità manutentive/assistenziali o di sicurezza (accesso effettuato previa esplicita autorizzazione del RPD e previa registrazione nel documento degli accessi informatici) e incidentalmente si dovessero riscontrare anomalie anche riguardanti la conservazione e nel trattamento dei dati/ informazioni ivi presenti, verranno presi gli opportuni provvedimenti e verrà effettuata segnalazione all'Autorità Giudiziaria in caso di riscontro di illeciti o violazioni.

Qualora il Dipendente, in presenza di deroga a quanto previsto nel presente paragrafo, abbia necessità di salvare e conservare una limitata quantità di dati e informazioni personali non inerenti l'attività lavorativa,



deve provvedere a salvare tali dati in un'apposita cartella creata dall'utente e denominata "Privatedocs - nome utente" (es. Privatedocs - Mario Rossi).

SANZIONI

È fatto obbligo a tutti i Dipendenti di osservare le disposizioni contenute nel presente Regolamento.

Il mancato rispetto o la violazione delle regole sopra citate, è perseguibile nei confronti del Dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL.

Nei confronti di collaboratori, consulenti, agenti e incaricati esterni, verificata la gravità della violazione contestata, si adotterà la risoluzione o il recesso dal contratto ad essi relativo, nonché tutte le azioni civili e penali previste.

Il presente Regolamento è soggetto a revisione periodica. La divulgazione della versione più recente della presente Policy avverrà con le modalità già descritte.