NORME GENERALI PER L'ACCESSO E L'USO DELLE RISORSE AZIENDALI

Oggetto del presente documento è l'individuazione delle norme da rispettare per l'accesso e l'uso delle risorse aziendali, in dotazione al personale dipendente e non, al fine di garantirne l'efficienza e la sicurezza dei processi di PRISMA s.r.l. rispetto agli standard internazionali ISO 9001:2015 e ISO 27001:2017.
Queste norme hanno lo scopo di conciliare le seguenti esigenze:
- da un lato il diritto del lavoratore/utente ad usare liberamente le tecnologie messe a disposizione (anche quale strumento di crescita professionale) ed il diritto al pieno rispetto della propria riservatezza
- dall'altro il diritto-dovere del Datore di lavoro di far sì che i dispositivi dati in dotazione alle proprie risorse non vengano usati in modo improprio;
- adeguarsi alla Normativa in materia di tutela dei dati personali Regolamento EU 679/2016 ed in particolare agli Artt. 29, 32 che prescrivono al Titolare del trattamento di istruire gli Addetti al trattamento e applicare le misure di sicurezza necessarie alla tutela dei dati personali.

CLASSIFICAZIONE DELLE INFORMAZIONI

Tutte le informazioni devono essere classificate secondo un livello adeguato che ne definisca il grado di riservatezza, integrità e disponibilità.

Riservatezza	L'accesso ai dati deve essere limitato in base ai privilegi indicati per gli utenti definiti, in accordo con il loro livello di classificazione. Le informazioni devono essere protette da eventuali accessi non autorizzati.
Integrità	Le informazioni devono essere complete e precise. Tutti i sistemi, gli asset e le reti devono funzionare correttamente, secondo specifiche che ne garantiscano la piena operatività.
Disponibilità	Le informazioni devono essere disponibili all'accesso e poter essere distribuite a chi ne detiene i diritti in base al livello di classificazione.

Tutti gli utenti interessati da questa disposizione devono trattare le informazioni in accordo con il livello di classificazione scelto.
I principi indicati da PRISMA s.r.l. per garantire riservatezza, integrità e disponibilità delle informazioni sono i seguenti:

- Ogni utente che venga in possesso di informazioni riservate è considerato responsabile della protezione delle stesse, soprattutto dall'accesso di terzi e dall'uso non autorizzato.
- Tutti gli utenti hanno la responsabilità di proteggere le loro password aziendali e altre credenziali di accesso collegate ad attività aziendali da un uso non autorizzato.
- Tutti gli accessi e l'utilizzo di informazioni riservate di proprietà di PRISMA s.r.l. devono essere autorizzate, per gli scopi connessi all'attività aziendale.
- I dipendenti e chiunque si trovi ad accedere a informazioni riservate di proprietà di PRISMA s.r.l. dovranno ricevere una adeguata formazione volta all'addestramento alla protezione delle stesse.
- Tutti gli utenti che utilizzano informazioni riservate appartenenti a PRISMA s.r.l. devono essere univocamente identificati.
- Le informazioni riservate devono essere protette su qualsiasi dispositivo aziendale.
- Le informazioni riservate devono essere protette anche nel caso l'utente le trasferisca su un dispositivo non aziendale. In tal caso il dispositivo dovrà seguire le regole per i dispositivi aziendali (es.: cellulare personale connesso alla emailaziendale).

NORME GENERALI PER L'ACCESSO E L'USO DELLE RISORSE AZIENDALI

- Tutti i server che memorizzano informazioni riservate appartenenti a PRISMA s.r.l. devono essere protetti da accessi non autorizzati.
- Tutti i dispositivi aziendali devono essere adeguatamente censiti e devono esserne note le loro ubicazioni fisiche abituali. Nel caso si verifichino spostamenti devono essere seguite le regole per il trasporto.
- I software vanno mantenuti aggiornati su tutti i dispositivi, in modo tale da garantire che le versioni correnti siano le più sicure.

Le informazioni sono classificati in funzione del valore, requisiti legali, sensibilità e criticità, le informazioni gestite dall'Organizzazione possono trovarsi in formato cartaceo e/o elettronico. Le informazioni si distinguono in:

Informazioni confidenziali: dati che non sono oggetto di divulgazione al pubblico. Documenti/informazioni specificatamente legate all'Organizzazione, al Sistema ed al suo funzionamento la cui divulgazione a soggetti non autorizzati potrebbe compromettere le attività lavorative e l'efficacia delle contromisure poste in essere nel Sistema Integrato di Gestione a protezione della disponibilità, integrità e riservatezza delle informazioni. I documenti che contengono questo tipo di informazioni sono classificati come "Confidenziali".

Informazioni riservate (uso interno): documenti/informazioni specificatamente legate all'Organizzazione, al Sistema ed al suo funzionamento la cui divulgazione non deve essere effettuata al di fuori di un ristretto insieme di addetti. I documenti che contengono questo tipo di informazioni sono classificati come "Riservati/Uso Interno".

Informazioni ad uso pubblico: documenti/informazioni specificatamente legate all'Organizzazione, al Sistema ed al suo funzionamento la cui divulgazione non compromette in alcun modo l'efficacia delle procedure poste in essere nel Sistema Integrato di Gestione; I documenti che contengono questo tipo di informazioni sono classificati come "Pubblici".

Tutte le informazioni derivate da contatti con i clienti, sono considerate informazioni fondamentali, accessibili solo a un uso interno, e sono pertanto classificate come riservate.

AMBITO DI APPLICAZIONE

Il presente regolamento si applica a ogni utente assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative della società.

Per utente pertanto si intende, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore, consulente, fornitore o altro che in modo continuativo non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.

Per azienda si intende, invece, la società, l'organizzazione e in generale il titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

NORME GENERALI PER L'ACCESSO E L'USO DELLE RISORSE AZIENDALI

I dispositivi informatici (personal computer fissi, portatili, tablet, smartphones, stampanti multifunzione: fotocopiatrice, scanner, fax; ecc..) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro il cui utilizzo ricade sotto la responsabilità del Titolare e che possono contenere dati riservati e informazioni personali di terzi. Vanno custoditi in modo appropriato evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone e possono essere utilizzati solo per fini professionali attinenti esclusivamente alle mansioni assegnate, evitando pertanto usi per fini personali, al di fuori dei casi consentiti ed autorizzati espressamente dai propri responsabili aziendali, tanto meno per scopi illeciti. Debbono essere prontamente segnalati all'azienda il furto, danneggiamento o smarrimento di tali strumenti. Le impostazioni dei dispositivi informatici sono predisposte dagli addetti informatici addetti sulla base di criteri e profili decisi dalla Direzione in funzione della qualifica del dipendente, delle mansioni cui questo è adibito, nonché dalle decisioni e della politica di utilizzo di tali strumenti stabilita dall'Azienda stessa.

È obbligo di tutto il personale dipendente e non, attenersi alla presente procedura, alle altre normative aziendali e alle disposizioni di legge in materia di trattamento di dati/informazioni (Privacy, etc.).

A tal fine si precisa sin d'ora che qualsivoglia dato o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'Azienda sarà dalla stessa considerata come avente natura aziendale e non riservata e/o personale della risorsa dipendente e non.
Premesso, quindi, che l'utilizzo delle risorse informatiche e l'utilizzo degli archivi cartacei della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, l'Azienda ha adottato il presente regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.
Si invita a tener ben presente che l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione da parte degli utenti assegnatari (dipendenti, collaboratori ecc.) al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli o scorrette che potrebbero esporre la società a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi. L'insieme delle norme comportamentali da adottare è ispirato ai principi di diligenza, informazione, correttezza nell'ambito dei rapporti di lavoro e inoltre finalizzato a prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti a essi attribuiti dall'ordinamento giuridico italiano. A tale proposito si rileva che gli eventuali controlli previsti escludono finalità di monitoraggio diretto e intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento (UE) 2016/679, alla legge n. 300/1970 (Statuto dei lavoratori) e ai provvedimenti emanati dall'Autorità Garante (in particolare Provvedimento del 1 marzo 2007).

SCHERMO E SCRIVANIA PULITI

"Schermo e scrivania puliti" significa trattare gli spazi di lavoro in modo tale per cui non siano mai visibili informazioni sensibili, anche in maniera accidentale. Al fine di proteggere tutti i dati sensibili e confidenziali PRISMA s.r.l. indica ai suoi dipendenti quali accorgimenti utilizzare affinché gli spazi di lavoro non rendano visibili informazioni sensibili. La postazione di lavoro è intesa come desktop, ma anche come scrivania, nel caso siano presenti documenti cartacei, e più in generale qualsiasi luogo nel quale siano contenute informazioni sensibili relative a PRISMA Srl, siano esse di proprietà dell'azienda, relative ai dipendenti, ai clienti o ai fornitori.

- La zona di lavoro deve essere costantemente presidiata, e resa sicura al termine della giornata di lavoro.

NORME GENERALI PER L'ACCESSO E L'USO DELLE RISORSE AZIENDALI

- Le postazioni computer devono essere bloccate o spente quando non utilizzate.
- I dati cartacei devono essere resi inaccessibili a terzi quanto non si è presenti alla postazione.
- Nel caso dei dati, in qualsiasi forma, vengano conservati in luoghi chiusi a chiave, le chiavi non devono mai essere lasciate incustodite.
- Le password non vanno mai scritte su foglietti lasciati accanto alla postazione di lavoro, e non vanno conservate in una posizione accessibile (anche un file sul computer non criptato è considerato accessibile).
- I computer vanno impostati in modo che automaticamente si blocchino e richiedano la password dopo più di cinque minuti di inutilizzo.

Nel caso il proprio cellulare o altri dispositivi siano connessi ad attività aziendali (es. email) le regole per la postazione si applicano anche a loro.

DISPOSITIVI (DEVICES): DESKTOP, LAPTOP, TABLET, SMARTPHONE, ETC.

Per l'espletamento delle proprie mansioni gli utenti utilizzano dispositivi (devices) di proprietà dell'ente e sono tenuti al rispetto delle seguenti regole:
• Non è consentito modificare la configurazione hardware e software del proprio dispositivo (device), se non previa esplicita autorizzazione dell'ente (per le modalità operative fare riferimento a quanto riportato all'art. 19 – Comunicazioni) che la esegue per mezzo dell'amministratore del sistema;
• Non è consentito rimuovere, danneggiare o asportare componenti hardware;
• Non è consentito installare autonomamente programmi informatici, applicativi e ogni altro software non autorizzato espressamente dall'ente;
• È onere dell'utente, in relazione alle sue competenze lavorative, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistema;
• È onere dell'utente spegnere il proprio PC al termine del lavoro. Per quanto concerne la gestione dei computer e degli altri dispositivi portatili, l'utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali files elaborati prima della loro riconsegna;
• Non è consentito all'utente caricare o inserire all'interno del computer o di altri dispositivi portatili qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare o almeno ridurre al minimo la possibile circolazione di dati personali sul medesimo apparecchio, gli utenti devono cancellare tutti quelli eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione.

DISPOSITIVI MOBILI DI CONNESSIONE (INTERNET KEY)

Agli assegnatari di computer o dispositivi portatili può essere concessa in dotazione anche una chiavetta per la connessione alla rete aziendale per consentire lo svolgimento delle mansioni lavorative anche da remoto. I suddetti dispositivi mobili di connessione devono essere utilizzati esclusivamente sui computer forniti in dotazione dall'ente e non è consentito concederne l'utilizzo a soggetti terzi né utilizzarli su altri computer sia personali che di terzi. Le specifiche relative ai limiti entro cui l'utente potrà utilizzare il servizio offerto tramite la chiavetta sono riportate nella scheda tecnica consegnata all'utente unitamente al dispositivo. L'utente dovrà attenersi ai suddetti limiti; in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.

NORME GENERALI PER L'ACCESSO E L'USO DELLE RISORSE AZIENDALI

DISPOSITIVI DI MEMORIA PORTATILI

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer: cd-rom, dvd, pen-drive USB, riproduttori musicali mp3, fotocamere digitali, dischi rigidi esterni, ecc.
L'utilizzo di tali supporti risponde alle direttive di seguito riportate:
• non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall'ente;
• è onere dell'utente custodire i supporti contenenti categorie particolari di dati (art. 9 GDPR) o dati relativi a condanne penali e a reati (art. 10 GDPR) in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato o distrutto.

Se autorizzati in base alle procedure previste, una volta connessi all'infrastruttura informatica dell'ente, i dispositivi saranno soggetti (ove ciò sia compatibile) al presente regolamento.

STAMPANTI, FOTOCOPIATRICI E FAX

L'utilizzo di tali strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte dell'ente.
Quando si inviano documenti contenenti dati personali o informazioni riservate su una stampante condivisa è richiesta una particolare attenzione; ciò al fine di evitare che persone non autorizzate possano venire a conoscenza del contenuto della stampa. Bisogna evitare quindi di lasciare le stampe incustodite e ritirare immediatamente le copie appena stampate.
L'utilizzo di fax per l'invio di documenti che hanno natura strettamente confidenziale è generalmente da evitare. In caso ciò sia necessario si deve preventivamente avvisare il destinatario in modo da ridurre il rischio che persone non autorizzate possano venire a conoscenza del contenuto della comunicazione e successivamente chiedere la conferma telefonica di avvenuta ricezione.
Gli strumenti dotati di memoria, connessi o meno in rete, sono gestiti dall'Amministratore di Sistema che provvede alla cancellazione periodica del loro contenuto e a tutte le operazioni ritenute necessarie per garantirne la sicurezza.

STRUMENTI DI FONIA MOBILE O DI CONNETTIVITÀ IN MOBILITÀ

A seconda del ruolo o della funzione del singolo utente, l'ente rende disponibili impianti di telefonia fissa e mobile e inoltre dispositivi quali smartphone e tablet che consentono di usufruire sia della navigazione in internet tramite rete dati che del servizio di telefonia tramite rete mobile.
Le specifiche relative ai limiti entro cui l'utente potrà utilizzare tali strumenti sono riportate nella scheda tecnica consegnata unitamente al dispositivo. L'utente dovrà attenersi ai suddetti limiti e in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.
Come per qualsiasi altra dotazione aziendale, il dispositivo mobile rappresenta un bene aziendale concesso in uso per scopi esclusivamente lavorativi.
È tuttavia permesso un utilizzo personale sporadico e moderato dei telefoni aziendali utilizzando la "diligenza del buon padre di famiglia" prevista dalla normativa e comunque tale da non ledere il rapporto fiduciario instaurato con il proprio datore di lavoro.
Al fine di controllo del corretto utilizzo dei servizi di fonia aziendale l'ente può esercitare i diritti di cui all'art. 124 D.Lgs. 196/2003 (fatturazione dettagliata) richiedendo ai provider di telefonia i dettagli necessari agli accertamenti sull'uso e relativo costo del traffico effettuato nel tempo.
I controlli saranno eseguiti secondo criteri e modalità descritte nel presente regolamento.

NORME GENERALI PER L'ACCESSO E L'USO DELLE RISORSE AZIENDALI

Qualora dall'esame del traffico di una singola utenza si rilevi uno scostamento significativo rispetto alla media del consumo sarà richiesto il tabulato analitico delle chiamate effettuate dalla SIM in incarico all'utente per il periodo interessato.

L'utilizzo dei dispositivi mobili risponde alle seguenti regole:
• Ciascun utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e conseguentemente, anche della sua diligente conservazione;
• I dispositivi devono essere dotati di password di sicurezza, per esempio codice PIN del dispositivo, che ne impedisca l'utilizzo da parte di altri soggetti. A tal fine si precisa che:
  - il codice PIN dovrà essere composto da quattro o cinque cifre numeriche, altri codici di accesso dovranno garantire analoga protezione; REGOLAMENTO PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA E DELLA RETE INTERNET
  - il codice PIN o altri codici di accesso dovranno essere modificato dall'assegnatario con cadenza al massimo semestrale;
  - ogni utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione all'ente.
• In caso di furto, danneggiamento o smarrimento del dispositivo mobile l'utente assegnatario dovrà darne immediato avviso all'ente; se tali eventi siano riconducibili a un comportamento negligente o imprudente dell'utente stesso o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;
• In caso di furto o smarrimento l'ente si riserva la facoltà di attuare la procedura di cancellazione da remoto di tutti i dati sul dispositivo, rendendo il dispositivo stesso inutilizzabile e i dati in esso contenuti del tutto irrecuperabili;
• Non è consentito all'utente caricare o inserire all'interno del dispositivo o SIM qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare o almeno ridurre la circolazione di dati personali sull'apparecchio, è obbligatorio cancellare tutti i dati eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione;
• Non è consentito all'utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi a meno che non siano strettamente connesse con il proprio compito lavorativo e siano preventivamente autorizzate dall'ente;
• L'installazione di applicazioni, gratuite o a pagamento, su smartphone e tablet deve essere espressamente autorizzata, rimanendo in caso contrario a carico dell'utente le responsabilità derivanti dall'installazione non autorizzata che costituisce violazione del presente regolamento;
• Salvo diversi specifici accordi derivanti da esigenze di servizio, al momento della consegna di tablet o smartphone l'utente è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli smartphone e tablet, consapevole che in caso contrario l'ente potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario.

GESTIONE DELLE COMUNICAZIONI TELEMATICHE –UTILIZZO DELLA RETE INTERNET

Ciascun utente potrà essere abilitato alla navigazione Internet e pertanto si richiamano tutti gli utenti a una particolare attenzione al suo utilizzo consapevole così come dei servizi collegati, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato all'ente.
La connessione a Internet, in quanto strumento a disposizione degli utenti per uso professionale, deve essere utilizzata in maniera appropriata, tenendo presente che ogni sito web può essere governato da

leggi diverse da quelle vigenti in Italia; ciò deve essere tenuto in considerazione in modo da prendere ogni precauzione conseguente.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:
• L'utilizzo è consentito esclusivamente per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
• Non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dall'ente;
• È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
• Non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in guest-book, anche utilizzando pseudonimi (o nicknames);
• Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica;
• È consentito l'utilizzo di soluzioni di Instant Messanger o chat esclusivamente per scopi professionali e attraverso strumenti e software messi a disposizione dall'ente;
• Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo;
• Non è consentito lo scambio o la condivisione di materiale audiovisivo, cinematografico, fotografico, informatico o altro anche se non protetto da copyright utilizzando sistemi Peer-toPeer, a qualsiasi titolo e anche se non a scopo di lucro.
• Non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata preventivamente ed espressamente approvata.

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere in qualunque modo essere nocivo all'immagine dell'ente. Per mezzo dell'Amministratore di Sistema e al fine di facilitare il rispetto delle predette regole l'ente si riserva la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti non consentiti, con esclusione dei siti istituzionali, e che prevengono operazioni non correlate all'attività lavorativa: a titolo esemplificativo e non esaustivo upload, restrizione nella navigazione, download di file o software.

GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE

Per ciascun utente titolare di un account, l'ente provvede ad assegnare una casella di posta elettronica individuale.
I servizi di posta elettronica devono essere utilizzati a scopo professionale: l'account e-mail è uno strumento di proprietà dell'ente ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.
Ad uno stesso utente possono essere assegnate più caselle di posta elettronica, che possono anche essere condivise con altri utenti dello stesso gruppo/ufficio/dipartimento. Tali caselle di posta elettronica devono essere utilizzate esclusivamente per la ricezione dei messaggi mentre per le risposte o gli invii deve sempre essere utilizzata la casella personale.
L'ente valuterà caso per caso, previa richiesta dell'utente, la possibilità di attribuire allo stesso un diverso indirizzo destinato ad uso privato. Attraverso le caselle e-mail aziendali gli utenti rappresentano pubblicamente l'ente e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere positivamente l'immagine aziendale. Gli utenti sono

responsabili del corretto utilizzo delle caselle di posta elettronica aziendale conformemente alle presenti regole.
Gli stessi devono:
• conservare la password nella massima riservatezza e con la massima diligenza;
• mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
• utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
• prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (agenti di alterazione, ad esempio virus);
• inviare preferibilmente files in formato PDF;
• accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i files attachment di posta elettronica prima del loro utilizzo;
• rispondere alle e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
• collegarsi a siti internet contenuti all'interno di messaggi solo per motivate ragioni e quando vi sia comprovata sicurezza sul contenuto degli stessi.
Inoltre, non è consentito agli utenti:
• diffondere il proprio indirizzo e-mail aziendale attraverso la rete internet;
• utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all'attività prestata in favore dell'ente, per esempio presentazioni o materiali video aziendali.
Salvo l'utilizzo di appositi strumenti di cifratura i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto si richiede agli utenti di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale".
Occorre infine che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute da altri nell'organizzazione di appartenenza del mittente. Nei casi in cui l'ente si doti di posta elettronica certificata si applicheranno, ove compatibili, le presenti disposizioni.

ACCESSO ALLA CASELLA DI POSTA ELETTRONICA DEL LAVORATORE ASSENTE

Saranno messe a disposizione di ciascun utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che in caso di assenze programmate consentano di inviare automaticamente messaggi di risposta contenenti le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore. In caso di assenze non programmate, ad esempio per malattia, qualora il lavoratore non possa attivare la procedura descritta anche avvalendosi di servizi webmail da remoto e perdurando l'assenza oltre il limite temporale di 7 (sette) giorni l'ente disporrà, lecitamente e mediante personale appositamente incaricato (l'Amministratore di Sistema oppure un suo incaricato), l'attivazione di un analogo accorgimento (risposta automatica o re-indirizzamento), avvertendo l'assente.

Nel caso in cui l'ente necessiti di conoscere il contenuto dei messaggi di posta elettronica dell'utente resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:
• la verifica del contenuto dei messaggi sarà effettuata per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato per iscritto dall'utente assente;

• di tale attività sarà redatto apposito verbale e informato l'utente interessato alla prima occasione utile.

CESSAZIONE DELL'INDIRIZZO DI POSTA ELETTRONICA AZIENDALE

In caso di interruzione del rapporto di lavoro con l'utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 (trenta) giorni da quella data ed entro 90 (novanta) giorni si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'ente si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie attività.

PASSWORD

La PRISMA s.r.l. considera la password, conformemente alle norme di sicurezza informatica, come una "informazione confidenziale di autenticazione composta da una serie di caratteri e/o simboli", utilizzata per l'accesso ai sistemi di elaborazione dell'informazione.
La struttura delle password individuata dall'utente presenta le seguenti caratteristiche informative e gestionali:

- obbligo di modifica al primo accesso;
- lunghezza minima di 8 caratteri;
- composizione con caratteri comprendenti almeno una lettera maiuscole, un carattere speciale e un numero;
- validità massima minore di 180 gg;
- non ripetibilità delle tre password precedenti;
- disattivazione automatica dopo 180 gg di non utilizzo.

SOFTWARE

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione dell'ente per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria, ad esempio freeware o shareware.ù
Il personale deve prestare attenzione ad alcuni aspetti fondamentali che ciascun utente è tenuto a osservare per un corretto utilizzo del software in azienda:
• Le licenze d'uso del software sono acquistate da vari fornitori esterni. L'utente è pertanto soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei rispettivi contratti di licenza.
• Non è consentito eseguire il download o l'upload di software non autorizzato.
• Considerato quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi soggette alle sanzioni previste dalla legge che comprendono il risarcimento del danno, il pagamento di multe e anche la reclusione.
• La duplicazione illegale del software non è giustificabile e non è tollerata, costituisce violazione del presente regolamento ed espone alle sanzioni disciplinari previste.

RISCHI

NORME GENERALI PER L'ACCESSO E L'USO DELLE RISORSE AZIENDALI

L'obiettivo è identificare e contrastare le possibili minacce alla sicurezza dei sistemi e delle informazioni della PRISMA s.r.l., al fine di predisporre adeguate misure di prevenzione e protezione.
Uno dei grandi rischi per la sicurezza delle informazioni di una organizzazione è rappresentato dal "codice malevolo" (malware: Virus, trojan, ecc.).
La strategia di PRISMA s.r.l. per la riduzione di questo rischio si basa su una serie di contromisure di natura preventiva, difensiva e di intervento per il contenimento del danno.
Le misure preventive adottate sono:

- Utilizzo di sistemi operativi progettati per la sicurezza, come GNU/Linux, Apple macOS, Microsoft Windows dalla versione 10 in poi.
- Mantenere aggiornati i sistemi operativi con l'ultimo livello di patch disponibile presso fonti affidabili e aggiornamenti automatici per macOS e Windows.

Le misure difensive adottate sono:

- Utilizzare e mantenere aggiornata la soluzione antivirus aziendale;

Le misure di intervento per il contenimento del danno sono:

- Isolare immediatamente i dispositivi su cui venga rilevato malware/virus.
- Disattivare le credenziali degli utenti potenzialmente violate a causa della compromissione del dispositivo.
- Ripristinare completamente il dispositivo compromesso evitando operazioni di recupero.

SICUREZZA LOGICA

Tutti gli utenti sono informati sugli ambiti di lavoro e sulla tipologia di informazioni a cui possono accedere. Ogni utente viene esplicitamente avvisato che il suo accesso è consentito solo alle aree di pertinenza formalmente autorizzate e documentate e, quindi, che eventuali accessi o tentativi di accesso ad aree non autorizzate potranno comportare provvedimenti nei suoi confronti. L'eventuale illecito nell'utilizzo delle informazioni aziendali e della strumentazione informatica da parte delle risorse, può generare in capo all'azienda una serie di responsabilità, sia penali sia civili, qualora l'azienda stessa non dimostri di aver adottato le "giuste" precauzioni. Gli utenti devono essere consapevoli del danno per l'azienda conseguente alla perdita di informazioni, loro alterazione e/o compromissione della riservatezza, causato da comportamenti inadeguati, fraintendimenti, errori nelle valutazioni, incuranza, disattenzione, stanchezza, mancanza di motivazione, ecc.
Gli utenti devono anche essere consapevoli del fatto che gli Amministratori di sistema hanno il diritto di accedere su tutti i sistemi, i computer e le apparecchiature aziendali e che l'azienda può raccogliere i "log" di tutte le transazioni, per gestire la qualità dei servizi informativi, per assicurare la rete aziendale, per garantire la sicurezza delle comunicazioni e la conformità alle normative, ai fini statistici e anche per controllare l'utilizzo delle risorse informative aziendali e il rispetto delle normative aziendali. Se un utente interno non rispetta le norme indicate in questo documento, i fatti rilevanti saranno portati all'attenzione della Direzione Aziendale, che valuterà i fatti.
L'azienda si riserva il diritto di esaminare tutte le informazioni conservate e trasmesse dai suoi sistemi e dalle sue reti. Questo monitoraggio può essere di natura globale, specifica o individuale. In caso di furto o smarrimento o danneggiamento di dispositivi mobili, e uso improprio degli stessi, non è esclusa a priori la responsabilità dell'utilizzatore nel sostenere, anche solo in parte, i costi per la riparazione o sostituzione del dispositivo mobile o di danni causati all'Azienda e ai propri clienti finali, e di cui l' Azienda dovrà rispondere di fronte a terzi.

Il personale dipendente e non della PRISMA s.r.l. deve accedere solo ai sistemi a cui sono stati autorizzati. Ogni abuso di accesso a sistemi diversi da quelli autorizzati, è perseguito ai sensi

dell'articolo 615-ter del Codice Penale "Accesso abusivo ad un sistema informatico o telematico", così come modificato dalla Legge 23 dicembre 1993 n. 547 "Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".
Qualora gli utenti dovessero accedere in modo incidentale a sistemi o ad applicazioni della PRISMA s.r.l. senza autorizzazione, sono tenuti a disconnettersi e segnalare l'anomalia al Responsabile IT.

CONTROLLI

L'ente esclude la configurabilità di forme di controllo aziendali aventi direttamente a oggetto l'attività lavorativa dell'utente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, statuto dei lavoratori).
Ciononostante non si esclude che si possano utilizzare sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro.
I controlli posti in essere saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati.
L'ente, riservandosi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici aziendali (artt. 2086, 2087 e 2104 c.c.), agirà in base al principio della gradualità.
In attuazione di tale principio:
• I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative;
• Nel caso in cui si dovessero riscontrare violazioni del presente regolamento, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite;
• In caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

SANZIONI

La violazione di quanto previsto dal presente regolamento, rilevante anche ai sensi degli artt. 2104 e 2105 c.c., potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 (sanzioni disciplinari) della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori).

Nel caso venga commesso un reato o la cui commissione sia ritenuta probabile o solo sospettata l'ente avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni o addebiti formali, le autorità competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.

In caso di violazione accertata delle regole e degli obblighi esposti in questo regolamento da parte degli utenti l'ente si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza o la funzionalità dei propri beni e strumenti informatici e inoltre per impedire il reitero di tale violazione.

INFORMATIVA AGLI UTENTI EX ART. 13 REGOLAMENTO (UE) 2016/679

NORME GENERALI PER L'ACCESSO E L'USO DELLE RISORSE AZIENDALI

Il presente regolamento, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici aziendali e relativamente al trattamento di dati personali svolti dall'ente finalizzato all'effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex art. 13 del Regolamento (UE) 2016/679

COMUNICAZIONI

Contestualmente all'assegnazione di un account il presente regolamento è messo a disposizione degli utenti per la consultazione. La versione più aggiornata dello stesso è pubblicata sia in formato immateriale digitale che in formato fisico cartaceo allo scopo di facilitarne la diffusione a tutti gli interessati.
Per ogni aggiornamento del presente regolamento sarà data comunicazione sulle bacheche aziendali e tramite l'invio di specifico messaggio e-mail e tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata. Le richieste di autorizzazione o concessione previste dal presente regolamento possono essere inoltrate all'ente per mezzo di qualsiasi strumento che ne garantisca la tracciabilità, ad esempio tramite e-mail, a cui è riconosciuto il valore di forma scritta in modo del tutto analogo rispetto a quella cartacea.

L'Amministratore

Prisma S.r.l.
Amministratore Unico
Dr. Salvatore Ribaudo