Versione 1 2019 02 14

POLITICA AZIENDALE SULLA SICUREZZA INFORMATICA

Premessa generale.

Il Titolare del Trattamento è ACMEI SUD S.P.A. Sede Legale, Direzione Generale e Uffici Amministrativi S.S.16 km 810.200 70019 Triggiano (Ba)

Il presente documento contiene le disposizioni, le misure organizzative e comportamentali che i dipendenti, i collaboratori a qualsiasi titolo dell'Azienda, sono chiamati ad osservare per contrastare i rischi informatici.

Premesso che l'utilizzo delle risorse informatiche e telematiche messe a disposizione da ACMEI SUD S.P.A. deve sempre ispirarsi al principio della diligenza e correttezza, con la presente Politica aziendale sulla sicurezza informatica s'intende contribuire alla massima diffusione della cultura della sicurezza in Azienda, evitando che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza dei sistemi informatici/informativi e nel trattamento dei dati. In particolare, il documento è suddiviso nelle seguenti due parti:

1. Regolamento sulle modalità di utilizzazione della strumentazione informatica messa a disposizione da ACMEI SUD S.P.A. per lo svolgimento dell'attività lavorativa e sulle relative procedure di controllo;

2. Norme comportamentali. Requisiti per i dipendenti, collaboratori esterni o individui con accesso a sistemi o dati.

Pubblicazione. Al presente documento - ed ai suoi futuri aggiornamenti - viene data massima diffusione attraverso la sua pubblicazione sul sito internet di Acmei Sud s.p.a..

1. Regolamento sulle modalità di utilizzazione della strumentazione informatica messa a disposizione da ACMEI SUD S.P.A. per lo svolgimento dell'attività lavorativa e sulle relative procedure di controllo.

Premessa. Il presente regolamento definisce le condizioni di utilizzo del Sistema informatico da parte dei collaboratori di ACMEI SUD S.P.A. attraverso gli strumenti messi a disposizione dall'Azienda, per il pieno ed efficace svolgimento delle attività proprie dell'amministrazione e dei servizi ad esse correlati. Tale Sistema informatico risponde ad usi ed obiettivi pubblici e aziendali e l'operatore che lo utilizza deve orientare il suo comportamento al perseguimento di tali scopi. L'utilizzo del Sistema è costantemente monitorato, nel rispetto della normativa sulla privacy e delle norme a tutela del lavoratore. Il regolamento prevede altresì un sistema sanzionatorio collegato all'uso improprio delle strumentazioni informatiche. Tutti i beni che ACMEI SUD S.P.A. mette a disposizione dei propri collaboratori per lo svolgimento dell'attività lavorativa devono essere utilizzati da parte di coloro che vi operano, a qualunque livello e con qualsiasi rapporto.

Principi generali. L'utilizzo degli strumenti informatici forniti ai collaboratori aziendali deve avvenire in modo strettamente pertinente all'attività lavorativa, in maniera lecita, appropriata, efficiente e razionale, tenendo sempre presente l'interesse collettivo al risparmio delle risorse. Deve altresì rispettare i principi etici e di correttezza nonché la privacy e la segretezza dei dati trattati secondo le normative vigenti. Il presente regolamento disciplina le modalità e finalità di utilizzo della strumentazione informatica, nonché le modalità di controllo di tale utilizzo, per garantire, nel rispetto della dignità e riservatezza delle persone in coerenza anche con la normativa vigente in materia di protezione dei dati personali (D.Lgs. n.196/2003 e successive modifiche ed integrazioni - Regolamento europeo 679/2016) e con quanto prescritto dal Garante per la protezione dei dati personali con la delibera n.13 del 1° marzo 2007, la sicurezza dei dati e del sistema informatico aziendale.

Destinatari. Sono destinatari del presente Regolamento tutti i collaboratori di ACMEI SUD S.P.A. con rapporto di lavoro subordinato (di qualsiasi tipologia) e coloro che svolgano, a qualsiasi titolo, attività per conto di ACMEI SUD S.P.A., accedendo al sistema informatico di quest'ultimo.

Modalità di utilizzo della strumentazione informatica. I destinatari si impegnano ad utilizzare la strumentazione informatica nel rispetto dei principi di cui al precedente punto e ad osservare le seguenti norme comportamentali: Utilizzo di Internet. L'accesso alla rete Internet fornita dall'Azienda è consentito esclusivamente per finalità lavorative e per l'accesso a dati ed informazioni concernenti l'attività aziendale; per motivi personali l'accesso è consentito soltanto in caso di necessità e comunque non in modo ripetuto o per periodi di tempo prolungati, evitando di: a. accedere a siti e/o acquisire e/o diffondere contenuti informativi osceni, o lesivi dell'onorabilità individuale o collettiva, o altro materiale potenzialmente offensivo o diffamatorio. In particolare è vietata la partecipazione ai social network (Facebook, MySpace, Twitter e simili), ai Blog, ai Forum di discussione, se ciò non è direttamente collegato alle attività lavorative rientranti nell'ambito della comunicazione esterna aziendale; rimanere collegati per periodi di tempo prolungati a siti musicali, anche se contestualmente si continua la propria attività lavorativa, in quanto ciò può appesantire il traffico della rete; d. scaricare programmi, anche gratuiti, se ciò non è indispensabile allo svolgimento dell'attività lavorativa, segnalandolo preventivamente al proprio responsabile o all'assistenza informatica; e. accedere a servizi con finalità ludiche o a chat line; f. accedere a siti per la condivisione e lo streaming di contenuti multimediali e simili, a meno che non si tratti di siti riconducibili all'attività lavorativa. Utilizzo del PC. In caso di allontanamento, anche

temporaneo, dalla postazione di lavoro, l'utente non deve lasciare il sistema operativo del proprio pc aperto e deve provvedere a proteggere il proprio computer attraverso la sospensione o il blocco della sessione di lavoro. Al termine dell'orario di servizio, prima di lasciare gli uffici, deve assicurarsi di avere opportunamente spento il proprio PC. L'utente è responsabile del PC portatile e/o eventuali accessori a lui assegnati (macchina fotografica, videoproiettore) e deve custodirli con diligenza, sia all'interno degli uffici, sia durante gli spostamenti esterni, fino alla loro riconsegna. Particolare attenzione deve essere prestata nell'utilizzo e nella custodia del PC portatile al di fuori della rete e degli uffici dell'Ente, (ad es. in telelavoro) nella connessione a reti esterne e nella rimozione di eventuali file personali memorizzati nel medesimo prima della riconsegna. Utilizzo delle stampanti e dei materiali di consumo. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali ecc…) è riservato esclusivamente all'attività lavorativa. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

Sicurezza e Privacy. Nell'utilizzo delle strumentazioni informatiche occorre adottare le seguenti cautele: a. mantenere segrete le proprie credenziali di autenticazione (password), sia quelle d'accesso alla strumentazione in dotazione sia quelle d'accesso ai vari programmi utilizzati nell'ambito della propria attività lavorativa, attribuite dal Responsabile del Sistema Informatico; b. non cedere, una volta autenticati nel proprio pc, l'uso della propria postazione a persone non autorizzate, in particolare per l'accesso ad internet ed ai servizi di posta elettronica; c. adottare, nello svolgimento della propria attività lavorativa, le necessarie cautele per assicurare la sicurezza dei dati trattati e dei dati che possono fornire indicazioni utili ad un eventuale "hacker" (attaccante dei sistemi informativi) dell'Azienda; d. utilizzare, in caso di trattamento di dati personali, le cartelle di rete o altri supporti di memorizzazione messi a disposizione dall'Azienda al fine di garantire la disponibilità dei dati anche a seguito di errori o eventi accidentali, grazie al sistema centralizzato di backup; e. prevedere opportune misure che consentano, in caso di assenza dal luogo di lavoro, ad altri utenti autorizzati l'accesso a dati potenzialmente necessari (per es. salvare i dati presenti sul proprio disco rigido in cartelle condivise su file server); f. non connettere alla rete interna dell'Azienda apparati esterni (come ad es. modem o router…) che possano compromettere il corretto funzionamento della rete aziendale; g. non utilizzare strumenti di messaggistica istantanea (per es. Skype, Messenger) per motivi personali; h. non introdurre o diffondere nella rete aziendale programmi illeciti (per es. virus, worm, spyware,...) ; i. non compiere azioni in violazione delle norme a tutela delle opere dell'ingegno e/o del diritto d'autore; j. utilizzare la posta elettronica messa a disposizione dell'ente per lo svolgimento dell'attività lavorativa, esclusivamente per le specifiche finalità della stessa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi; k. non utilizzare mail esterne in software di posta elettronica (es. Outlook Express), in quanto le stesse comportano rischi per la sicurezza dei sistemi, mentre è consentito l'utilizzo a fini privati di mail esterne via web (es. googlemail, poste.it, alice…), purché con moderazione e per brevi periodi di tempo; l. aver cura di non aprire allegati di posta in e-mail dal mittente e/o dall'oggetto sospetti per prevenire i rischi causati da software nocivi (per es. virus, worm, spyware, ecc.); m. limitare al minimo indispensabile la diffusione del proprio indirizzo di e-mail istituzionale su siti web pubblici (per es. forum, mailing list, ecc.); n. non rimuovere il programma antivirus installato sulla postazione di lavoro; o. verificare la presenza di eventuali virus prima di utilizzare supporti rimovibili; p. nel caso in cui il software antivirus rilevi la presenza di un virus sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'evento all'assistenza informatica; non inviare messaggi di posta elettronica contenenti segnalazioni del virus ad altri utenti; q. utilizzare sulle postazioni di lavoro esclusivamente il software autorizzato e fornito dall'Azienda; eventuali software aggiuntivi, rispetto all'installazione standard, dovranno essere richiesti al proprio responsabile; r. non lasciare incustoditi i dispositivi mobili aziendali (come ad esempio i cellulari e i tablet aziendali); s. in caso di incidente di sicurezza (come ad esempio nei casi di accesso non autorizzato o di minacce informatiche al sistema), attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi; t. Nell'utilizzo della posta elettronica certificata, le credenziali (user id e password) per accedere a tale casella di posta devono essere a conoscenza unicamente dei collaboratori dell'ufficio autorizzati dal responsabile del servizio.

Controlli. L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento, nonché nel rispetto dello Statuto dei Lavoratori. I controlli vengono effettuati dal Responsabile della sicurezza con l'ausilio dell'assistenza tecnica.

Principi. L'Azienda ritiene che l'attività di prevenzione debba essere prevalente rispetto all'attività di controllo. Si impegna pertanto a potenziare in misura crescente tale attività di prevenzione, in particolare tramite azioni di sensibilizzazione e di diffusione dei principi e delle regole da osservare nell'utilizzo della strumentazione informatica, nell'adozione di specifiche soluzioni tecnologiche e di ogni altra misura ritenuta idonea a tal fine. I controlli effettuati dall'Azienda rispettano i seguenti principi: a) necessità: i dati trattati durante l'attività di controllo sono sempre e soltanto quelli strettamente necessari a perseguire le finalità esposte nei paragrafi precedenti; b) proporzionalità: i controlli sono sempre effettuati con modalità tali da garantire, nei singoli casi concreti, la pertinenza e non eccedenza delle informazioni rilevate rispetto alle finalità perseguite; c) imparzialità: i controlli sono effettuati su tutta la strumentazione informatica messa a disposizione dall'amministrazione aziendale e conseguentemente possono coinvolgere tutti i collaboratori della stessa, a qualunque titolo utilizzino tale strumentazione, fatta eccezione per quella assegnata alle rappresentanze sindacali unitarie e agli organi istituzionali. In nessun caso sono effettuati controlli mirati e ripetuti nei confronti di soggetti specifici con finalità discriminatorie o persecutorie o volutamente sanzionatorie; d) trasparenza: in base a tale principio l'amministrazione mette in atto tutte le azioni necessarie a garantire la preventiva conoscenza da parte di tutti i soggetti potenzialmente sottoposti ai controlli del presente regolamento. Sono pertanto informati dei possibili controlli tutti i soggetti di cui al precedente punto "destinatari"; e) protezione dei dati personali: i controlli sono in ogni caso effettuati rispettando la dignità e la libertà personale dei soggetti sottoposti a controllo, nonché garantendo la riservatezza dei dati personali raccolti durante la procedura di controllo. I dati sono conosciuti soltanto dai soggetti preventivamente designati quali responsabili e incaricati del trattamento. Oltre a quanto specificato

sopra, i controlli sono effettuati rispettando la normativa vigente in materia di protezione dei dati personali.

Finalità. I controlli di cui al presente regolamento sono effettuati per le seguenti finalità: a) evitare che vengano compiuti comportamenti impropri e/o potenzialmente dannosi per l'Amministrazione che possano comportare anche l'irrogazione di sanzioni disciplinari; b) evitare o comunque ridurre i rischi di un coinvolgimento civile e penale dell'Azienda, per concorso di reato, nel caso di illeciti nei confronti di terzi commessi mediante l'utilizzo improprio dei beni messi a disposizione dall'Amministrazione stessa; c) tutelare l'immagine dell'Azienda e di coloro che vi prestano la propria attività.

Modalità di effettuazione dei controlli. Il controllo è effettuato su strumentazioni informatiche determinate a seguito di specifica segnalazione effettuata da un soggetto terzo oppure a seguito ad una verifica di sicurezza. Nel caso in cui la segnalazione del soggetto terzo si riferisca a una persona nominativamente individuata, il Responsabile della sicurezza dell'Azienda deve dare informazione di tale controllo al a tale soggetto. Le segnalazioni di un soggetto terzo sono ritenute più attendibili qualora non siano anonime e rivolte per iscritto al Responsabile della sicurezza. La verifica di sicurezza consiste in una attività di controllo da parte del Responsabile della sicurezza, il quale, dopo aver rilevato elementi che possano configurare un utilizzo improprio delle strumentazioni informatiche, anche mediante ulteriori accertamenti, comunica i dati strettamente necessari, acquisiti attraverso tale controllo, al Responsabile dell'Ufficio di appartenenza del collaboratore interessato. Quest'ultimo potrà effettuare le ulteriori valutazioni e adottare le azioni conseguenti. Gli ulteriori accertamenti sopraindicati possono ricomprendere controlli sui log (siti di navigazione in Internet). E' possibile verificare il contenuto dei siti di navigazione soltanto nel caso in cui le relative informazioni siano indispensabili al fine di rilevare un utilizzo proprio o improprio dello strumento informatico. Qualora, anche a seguito delle ulteriori verifiche effettuate, il Responsabile della sicurezza riscontri elementi che confermino un possibile uso improprio delle strumentazioni messe a disposizione dall'Azienda, associa il nominativo dell'utilizzatore alla postazione client, per poter procedere come di seguito disciplinato. Conseguentemente alle verifiche sopraindicate e all'individuazione del nominativo dello/degli utilizzatore/i, il Responsabile della sicurezza - trasmette al dirigente di riferimento del soggetto coinvolto un "Verbale di controllo" affinché il dirigente stesso possa effettuare le valutazioni conseguenti, con particolare riferimento ad una verifica relativa alla pertinenza (o stretta attinenza) dei dati di navigazione, trasmessi nel Verbale stesso, con l'attività lavorativa; - ne dà contestuale comunicazione al soggetto coinvolto. La verifica di pertinenza con l'attività lavorativa, effettuata dal dirigente di riferimento, deve comprendere anche una tempestiva audizione del soggetto controllato, affinché quest'ultimo possa fornire chiarimenti, motivazioni ed osservazioni in merito a quanto rilevato. Alla audizione può essere presente, su richiesta del dirigente di riferimento o del soggetto coinvolto nel controllo, il Responsabile della sicurezza (o altro tecnico addetto alla sicurezza individuato dal Responsabile della sicurezza). A seguito delle verifiche sopra specificate, il dirigente comunica immediatamente per iscritto all'utilizzatore l'esito del controllo e adotta nel contempo le opportune misure tecniche/organizzative per evitare il ripetersi del comportamento anomalo, richiamandolo, qualora emergano sue responsabilità. Nel caso in cui dall'accertamento emerga un uso gravemente improprio della strumentazione informatica, il dirigente avvia il conseguente procedimento disciplinare.

2. Norme comportamentali. Requisiti per i dipendenti, collaboratori esterni o individui con accesso a sistemi o dati.

È dovere dei dipendenti completare il corso di formazione di sulla sensibilizzazione in materia di sicurezza informatica e sostenere le policy di utilizzo accettabile. Qualora si notasse un individuo non identificato, non accompagnato o non autorizzato all'interno dell' Azienda, informare immediatamente il proprio diretto superiore. I visitatori devono essere sempre accompagnati da un dipendente autorizzato. Chi riveste l'incarico di accompagnatore deve accertarsi che i visitatori si limitino alle aree autorizzate. È vietato fare qualsiasi riferimento al soggetto o al contenuto dei dati sensibili o riservati in ambito pubblico o su sistemi o canali di comunicazioni non controllati dall'Azienda. È ad esempio vietato diffondere dati mediante sistemi di posta elettronica il cui hosting non viene fornito dall'Azienda. Tenere ordinata la scrivania. Per proteggere le informazioni è necessario accertarsi che i dati, in formato stampato, rientranti in questo campo di applicazione non vengano lasciati esposti o incustoditi sulle workstation. È richiesto l'uso di una password sicura su tutti i sistemi di aziendali come indicato nella policy di utilizzo delle password. Le credenziali devono essere uniche e diverse da quelle utilizzate per sistemi o servizi esterni. Al termine del contratto lavorativo, i dipendenti hanno l'obbligo di restituire qualsiasi record, in qualsivoglia formato, che contenga informazioni personali. Informare immediatamente l'amministratore di sistema in caso di smarrimento di un dispositivo (per es. telefoni cellulari, laptop, ecc...) contenente dati di tale natura. Qualsiasi dipendente sospetti che un sistema o un processo non rispetti la compliance a questa policy ha l'obbligo di informare l'amministrazione di sistema, per consentire l'adozione delle necessarie misure correttive. Qualsiasi utente a cui sia stata concessa la possibilità di lavorare in remoto deve adottare ulteriori precauzioni, allo scopo di garantire un'adeguata gestione dei dati. Accertarsi che le risorse contenenti dati appartenenti a questo campo di applicazione non vengano esposte a rischi inutili; evitare ad esempio di lasciarle in vista nel sedile posteriore dell'auto. Per trasferire dati entro il perimetro Aziendale utilizzare esclusivamente meccanismi sicuri forniti dall'azienda stessa (per es. chiavi USB, condivisioni file ed e-mail cifrate, ecc...). A questo scopo l'Azienda metterà a disposizione appositi sistemi o dispositivi. È vietato utilizzare altri meccanismi per la gestione dei dati che rientrano in questo campo di applicazione. Qualora aveste domande relative al meccanismo di trasferimento, o nel caso in cui tale procedura ostacolasse le vostre mansioni lavorative, è vostro dovere discuterne con l'Amministratore di sistema. Qualsiasi informazione in procinto di essere trasferita su un dispositivo mobile (per es. chiave USB o laptop) deve essere cifrata, in conformità con best practice di settore, leggi e normative vigenti. Se fosse presente qualsivoglia incertezza sui suddetti requisiti, richiedere consulenza all'Amministratore di sistema.