Regole sull'uso della strumentazione informatica e della rete internet

Allegato 4 al "Manuale di gestione documentale"

CAPO I – PRINCIPI

Art. 1 – Introduzione, Definizioni e Finalità

Il presente documento disciplina l'uso degli strumenti informatici (postazioni di lavoro fisse e mobili, smartphone, tablet, posta elettronica e rete Internet e Intranet) che l'Automobile Club Roma (di seguito "AC" o "Ente") mette a disposizione dei dipendenti e degli utenti, al fine di assicurare la corretta e adeguata gestione del patrimonio informativo aziendale, la tutela dei dati personali e la sicurezza dei sistemi informativi.

Il documento tiene conto delle linee guida fornite dall'Autorità Garante per la Tutela dei Dati Personali con Provvedimento del 1° marzo 2007, del Regolamento (UE) n. 2016/679 (GDPR) e del Decreto Legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) ed è finalizzato ad assicurare la sicurezza dei sistemi informativi in uso presso l'Ente.

Il presente documento tiene conto, altresì, delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, nonché delle buone pratiche indicate nel Framework Nazionale per la Cybersecurity.

Considerata la dimensione contenuta dell'infrastruttura informatica dell'Ente – costituita da un numero limitato di postazioni, un server locale e risorse condivise – le misure tecniche e organizzative previste dal presente Regolamento sono da ritenersi adeguate e proporzionate ai sensi dell'art. 32 del Regolamento (UE) 2016/679, anche in ragione del rischio limitato di esposizione a minacce gravi o diffuse.

Art. 2 – Ambito di applicazione

Il presente documento si applica a ogni utente assegnatario di beni e risorse informatiche dell'AC ovvero utilizzatore di servizi e risorse informative.

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

Art. 3 – Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi ICT e le reti informative, a qualunque titolo detenute (proprietà, noleggio, comodato, ecc.) sono da considerarsi beni di pertinenza dell'Ente.

Il loro utilizzo è consentito all'utente esclusivamente per fini professionali.

Ogni dato o informazione trattata dall'utente per mezzo dei beni e delle risorse informatiche messe a disposizione dall'Ente è considerato

come avente natura non privata né riservata.

Art. 4 – Responsabilità personale dell'utente

Ogni utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidategli dall'Ente nonché dei dati trattati.

A tal fine l'utente è tenuto a tutelare il patrimonio utilizzato da utilizzi impropri o non autorizzati, danni o abusi, anche derivanti da negligenza, imprudenza o imperizia.

L'utente è tenuto a operare a tutela della sicurezza informatica, in relazione al proprio ruolo e alle attività svolte, riportando senza ritardo al Direttore dell'Ente eventuali rischi di cui è a conoscenza ovvero violazioni, anche solo potenziali, alle disposizioni di cui al presente Regolamento.

Art. 5 – Controlli

In conformità all'art. 4, comma 1 della legge 300/1970, la regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro, ma solo a permettere a quest'ultimo di utilizzare i sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

Gli eventuali controlli effettuati sull'utilizzo delle risorse informatiche escludono finalità di monitoraggio diretto e intenzionale dell'attività lavorativa, e sono disposti esclusivamente nel rispetto della normativa vigente, con particolare riferimento alla legge 20 maggio 1970, n. 300 (Statuto dei lavoratori).

Viene, in ogni caso, assicurato al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Regolamento Europeo 2016/679 (GDPR).

Nel rispetto di tali disposizioni, l'AC ha facoltà di effettuare controlli saltuari e occasionali per verificare l'integrità del sistema informativo e assicurare l'ordinaria manutenzione dello stesso, riservandosi in tale sede di accertare e segnalare eventuali abusi e/o violazioni commessi dall'utente.

Parimenti, l'AC potrà in qualsiasi momento procedere alla rimozione di ogni file, applicazione, account personale di cui fosse venuto a conoscenza.

In ogni caso, l'AC si impegna a rispettare i principi di proporzionalità, pertinenza e non eccedenza nelle attività di controllo, non utilizzando apparecchiature hardware o software al fine di svolgere controlli costanti, prolungati o indiscriminati nei confronti degli utenti.

Capo II — MISURE ORGANIZZATIVE

Art. 6 – Amministratori di sistema

Il Direttore dell'AC è "Amministratore di sistema" secondo il Regolamento europeo 679/16 (GDPR)" e il Provvedimento Generale dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

L'Amministratore di sistema, anche avvalendosi della assistenza specialistica di ACI Informatica e dell'assistenza delle competenti strutture dell'ACI, ha il compito di sovrintendere ai beni e alle risorse informatiche dell'Ente, curando di:

- gestire l'hardware e il software di tutta la strumentazione informatica di cui l'Ente è titolare;
- gestire la creazione, l'attivazione, la disattivazione degli account per l'accesso alla rete e dei relativi privilegi di accesso alle risorse;
- monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti;
- creare, modificare, rimuovere o utilizzare qualunque account o privilegio nell'ambito delle attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- installare o rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti;
- svolgere gli interventi necessari per tutelare la sicurezza informatica dei sistemi informativi.

Art. 7 – Assegnazione degli account e gestione delle password

7.1 – *Creazione e gestione degli account*

Un "**account**" è l'insieme di dati e credenziali che identificano in modo univoco un utente all'interno di un sistema digitale, consentendogli di accedere a servizi, funzionalità e contenuti personalizzati.

Gli account vengono creati dagli amministratori di sistema e sono personali, cioè associati univocamente alla persona assegnataria. Ogni utente è personalmente responsabile dell'utilizzo del proprio account.

L'accesso al proprio account avviene tramite l'utilizzo delle "**credenziali di autenticazione**", solitamente username e password, comunicate all'utente dall'amministratore di sistema che le genera con modalità tali da garantirne la segretezza.

L'utente è tenuto a mantenere strettamente personali e riservate le credenziali di autenticazione, con divieto di comunicarne gli estremi a terzi.

Qualsiasi operazione effettuata attraverso l'inserimento di credenziali identificate dal sistema informatico di riconoscimento (quale il codice utente associato alla parola chiave riservata) si presume svolta dal titolare delle medesime credenziali, indipendentemente dalla postazione di lavoro utilizzata, salvo che lo stesso non fornisca prova contraria.

Se l'utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da terzi o che sia comunque, anche solo potenzialmente, possibile l'accesso non autorizzato ad account personali, è tenuto a modificare immediatamente la password e a segnalare la violazione all'Amministratore del sistema.

In caso di assenza improvvisa o prolungata del lavoratore, l'Ente si riserva la facoltà di accedere a qualsiasi dotazione o apparato assegnato in uso all'utente, al fine di assicurare le esigenze di lavoro garantire la sicurezza e operatività delle risorse informatiche.

7.2 – *Gestione e Utilizzo delle Password*

A seguito della prima comunicazione delle credenziali di autenticazione l'utente ha il compito di modificare la password personale al primo utilizzo e almeno ogni 6 mesi.

L'utente, nel definire la password, deve rispettare le seguenti regole:

- utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, ecc.), di cui almeno uno numerico;
- includere nella password almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "@#$£$%...";
- evitare di impostare la password con nome, cognome, data di nascita o, comunque, elementi agevolmente a lui riconducibili;
- evitare l'utilizzo di password comuni o prevedibili;
- proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

È rigorosamente vietato riportare la password su post-it o altri supporti cartacei.

7.3 – *Cessazione Degli Account*

In caso di cessazione del rapporto lavorativo gli account sono disattivati.

7.4 *Autenticazione multifattoriale (2FA/MFA)*

Laddove tecnicamente possibile, l'accesso ai sistemi informatici, alle caselle PEC e alle piattaforme documentali deve essere protetto da un sistema di autenticazione forte (secondo fattore), in conformità alle Linee Guida AgID e alle best practice di sicurezza.

Art. 8 – Postazioni di lavoro

Per "postazione di lavoro" si intende il complesso unitario di personal computer (di seguito pc), notebook, tablet, smartphone, accessori, periferiche e ogni altro dispositivo (device) concesso in utilizzo all'utente. L'assegnatario di tali beni e strumenti informatici ha l'obbligo di farne un uso limitato alle attività di servizio.

Salvo diversa decisione, l'AC Roma si avvale di "postazioni di lavoro" acquisite in noleggio nel quadro dei servizi resi disponibili agli Automobile Club provinciali dall'ACI attraverso il contratto ***Integra***.

Ogni postazione di lavoro, a prescindere dal titolo di possesso in capo

all'Ente, rimane nella sua esclusiva titolarità ed è concessa all'utente per lo svolgimento delle proprie mansioni lavorative per finalità attinenti all'attività svolta.

Ad ogni dipendente in servizio è assegnata una postazione di lavoro fissa; è facoltà dell'Amministrazione assegnare postazioni mobili, anche in alternativa alla postazione fissa; è responsabilità del dipendente usare le postazioni in modo protetto ed esclusivamente per motivi di servizio.

È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a terzi.

L'utente ha l'obbligo di usare i computer e gli altri dispositivi a lui affidati responsabilmente, professionalmente e nel rispetto delle regole di sicurezza informatica.

Gli apparecchi di proprietà personale dell'utente, quali computer portatili, telefoni cellulari, smartphone, agende palmari, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali e qualsiasi altro dispositivo non possono essere utilizzati per le attività di servizio, salvo preventiva autorizzazione dell'Amministratore di sistema. In tal caso essi sono soggetti alle disposizioni del presente documento.

L'utente deve segnalare con la massima tempestività all'Amministratore di sistema eventuali guasti, malfunzionamenti e anomalie tecniche rilevate.

In casi eccezionali, e solo previa autorizzazione dell'Amministratore di sistema, può essere consentito l'uso controllato di dispositivi personali per esigenze operative, a condizione che siano preventivamente configurati secondo gli standard di sicurezza dell'Ente.

CAPO III – REGOLE DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 9 – Misure sull'utilizzo dei dispositivi.

Per l'espletamento delle proprie mansioni gli utenti, nell'uso dei dispositivi assegnati dall'Ente, sono tenuti al rispetto delle seguenti regole:

- non è consentito modificare la configurazione hardware e software del dispositivo assegnato se non previa esplicita autorizzazione dell'Amministrazione di sistema;
- non è consentito rimuovere, danneggiare o asportare componenti hardware;
- non è consentito installare, modificare, duplicare o rimuovere autonomamente software o applicazioni senza preventiva autorizzazione dell'Amministrazione di sistema;
- non è consentito utilizzare il software installato oltre i limiti specificati nei contratti di licenza;
- non è consentito eseguire il download o l'upload di software, senza preventiva autorizzazione dell'Amministrazione di sistema.

- è onere dell'utente mantenere aggiornato il software installato sulla propria postazione di lavoro nonché sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto all'Amministratore del sistema;
- è vietato lasciare le postazioni di lavoro incustodite con le sessioni utente attive. L'utente, in caso di allontanamento anche temporaneo dalla propria postazione di lavoro, è tenuto a bloccare la tastiera (Ctrl+Alt+Canc) e lo schermo con un programma salvaschermo (screensaver) protetto da password ed effettuare il log-out dalle sessioni eventualmente attive.
- è onere dell'utente assumere comportamenti tali da ridurre il rischio di attacco al sistema informativo aziendale;
- è obbligatorio controllare costantemente la presenza, l'aggiornamento e il regolare funzionamento del software antivirus aziendale e sospendere le attività in presenza di messaggi indicanti software malevoli (cd. malware), informando tempestivamente l'Amministratore di sistema;
- non è consentito all'utente caricare all'interno del computer o di altri dispositivi portatili qualsiasi dato personale non attinente con l'attività lavorativa svolta.

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.

In caso di furto o smarrimento di strumenti informatici dell'Amministrazione, l'utente affidatario è tenuto a denunciare l'accaduto all'Autorità di Pubblica Sicurezza e a darne tempestivamente comunicazione al Direttore per l'adozione delle opportune misure, con riguardo alla sicurezza dei dati e dei sistemi e alla tutela dei dati personali.

L'Ente utilizza un **server locale** per la gestione documentale interna e la condivisione di file tra le UOR, mediante cartelle condivise ad accesso controllato. L'uso di tali cartelle è consentito esclusivamente per finalità di servizio e nel rispetto delle regole di riservatezza, integrità e autorizzazione all'accesso definite nel presente documento e delle policy organizzative dell'Ente.

Art. 10 – Dispositivi di memoria portatili

Per dispositivi di memoria portatili si intendono gli apparati che consentono di archiviare e utilizzare files all'esterno del PC, quali CD-Rom, DVD, Pen-drive USB, riproduttori musicali mp3, fotocamere digitali, dischi rigidi esterni, ecc.

In considerazione dei rischi intrinseci connessi alla trasmissione di malware, è consentito utilizzare tali dispositivi solo qualora siano anch'essi forniti in dotazione dall'Ente.

È onere dell'utente custodire i supporti contenenti dati personali, 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 e, comunque, attenersi alle misure stabilite dall'Ente per la minimizzazione del rischio riferito al processo di riferimento, curando sempre di cancellare i dati la cui conservazione non sia necessaria.

Art. 11 – Uso di strumenti cloud e archiviazione esterna

I dipendenti dell'Ente possono utilizzare esclusivamente la piattaforma Google Drive integrata con il servizio di posta elettronica aziendale fornito da Google, per l'archiviazione, condivisione e trattamento dei documenti elettronici.

È vietato l'uso di qualsiasi altra piattaforma cloud (es. Dropbox, OneDrive, iCloud, ecc.) non autorizzata, anche se ad accesso personale, per scopi legati all'attività lavorativa dell'Ente.

L'utilizzo di Google Drive deve comunque avvenire nel rispetto dei principi di riservatezza, integrità e disponibilità delle informazioni, e secondo le indicazioni fornite nel presente Regolamento e nelle policy aziendali.

Art. 12 – Periferiche per la trasmissione o acquisizione di documenti e documenti cartacei

L'utilizzo di periferiche di digitalizzazione, ricezione e invio di documenti cartacei (quali stampanti, scanner, fotocopiatrici e fax) è consentito esclusivamente per ragioni di servizio.

Nel caso di trasmissione alle periferiche di documenti contenenti dati personali o informazioni riservate, l'utente deve adottare le cautele necessarie al fine di evitare che persone non autorizzate possano venire a conoscenza del loro contenuto.

L'utilizzo del fax non è consentito.

Fermo restando quanto previsto dal presente documento, il contenuto digitale dei documenti acquisiti o trasmessi mediante periferiche deve essere prontamente cancellato dopo l'uso.

È vietato lasciare stampe incustodite e non ritirate dall'interessato.

Analogamente, è onere di ciascun utente allontanarsi dal proprio posto di lavoro senza aver adottato le misure a tutela della protezione dei dati personali con riferimento a documenti cartacei lasciati incustoditi e non opportunamente archiviati.

Art. 13 – Apparati per la fonia mobile o la connettività in mobilità - Smartphone

A seconda del ruolo o della funzione dell'utente, l'Ente rende disponibili impianti di telefonia fissa e mobile e dispositivi, quali smartphone e tablet, che consentono di usufruire sia della navigazione in Internet che del servizio di telefonia in mobilità.

Le prescrizioni di utilizzo di tali strumenti sono riportate nella scheda tecnica consegnata unitamente al dispositivo.

Il dispositivo mobile rappresenta un bene aziendale concesso in uso

per scopi esclusivamente di servizio. È tuttavia permesso l'uso privato nell'ambito del servizio di *dual billing*, che consente al dipendente di effettuare, a proprie spese, chiamate di carattere personale.

Al fine di controllare il 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.

Qualora dall'esame del traffico di una singola utenza si rilevi uno scostamento significativo rispetto alla media del consumo, il Direttore potrà acquisire il tabulato analitico delle chiamate effettuate dalla SIM assegnata 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, che ne impedisca l'utilizzo da parte di altri soggetti. A tal fine si precisa che:
    - il codice PIN dovrà essere conforme alle specifiche fissate dal produttore del modello utilizzato;
    - 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.

In caso di furto o smarrimento del dispositivo, l'utente affidatario è tenuto a denunciare l'accaduto all'Autorità di Pubblica Sicurezza e a darne tempestivamente comunicazione al Direttore per l'adozione delle opportune misure, anche con riguardo alla tutela dei dati. L'Ente si riserva la facoltà di attuare il blocco da remoto di tutti i dati sul dispositivo, rendendo lo stesso inutilizzabile e i dati in esso contenuti 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 la diffusione di dati personali, è obbligatorio cancellare tutti i dati eventualmente presenti prima di consegnare il dispositivo per la restituzione o la riparazione.

L'installazione di applicazioni, gratuite o a pagamento, su smartphone e tablet aziendali è consentita esclusivamente previa autorizzazione dell'Amministratore di sistema. In assenza di tale autorizzazione, ogni responsabilità derivante dall'installazione ricade integralmente sull'utente.

Capo IV — GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 14 – Gestione utilizzo della rete Internet

Ciascun utente è abilitato alla navigazione sulla rete Internet mediante l'indirizzo Internet pubblico assegnato all'Ente ed è, pertanto, è tenuto ad osservare particolare attenzione al suo utilizzo, consapevole dei rischi connessi.

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 alla rete Internet resa disponibile dall'Ente sono le seguenti:

- l'utilizzo è consentito esclusivamente per finalità di servizio e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle stesse;
- non è consentita l'effettuazione di transazioni finanziarie, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo che per ragioni di servizio;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- non è permessa, 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 se non per ragioni di servizio;
- salvo che nei casi di materiale afferente a iniziative istituzionali, non è consentito lo scambio o la condivisione di files audiovisivi, cinematografici, fotografici, informatici o altro, anche se non protetto da copyright, utilizzando sistemi Peer-to- Peer, a qualsiasi titolo e anche se non a scopo di lucro.
- non è consentito sfruttare marchi registrati, segni distintivi e ogni altro bene immateriale di proprietà dell'Ente in pagine web o pubblicandoli su Internet, a meno che tale azione non sia stata preventivamente ed espressamente autorizzata;
- è consentita l'effettuazione di adempimenti on line nei confronti di Pubbliche Amministrazioni e di concessionari di servizi pubblici, o

per tenere rapporti con istituti bancari e assicurativi, nei tempi strettamente necessari allo svolgimento delle transazioni, come indicato nella Direttiva n° 2 del 26 maggio 2009 emanata dal Ministro per la Pubblica Amministrazione e l'Innovazione;
- è vietato effettuare download di file musicali o multimediali, se non previa autorizzazione;

È altresì rigorosamente vietato qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere in qualunque modo essere nocivo all'immagine dell'ente.

Sono fatte salve le disposizioni del Codice di Comportamento dell'Ente.

Art. 15 – Posta elettronica ordinaria personale

15.1 – *Regole sull'utilizzo della posta elettronica*

Ad ogni utente viene fornito un account e-mail nominativo, conforme, per i dipendenti, alla sintassi **[iniziale del nome].cognome@aciroma.it**.

La casella di posta elettronica ordinaria (PEO) istituzionale è uno strumento di lavoro e pertanto, l'assegnatario è responsabile del suo corretto utilizzo.

La "personalizzazione" dell'indirizzo non comporta il suo carattere "privato", in quanto trattasi di strumento di esclusiva proprietà dell'AC, messo a disposizione del dipendente al solo fine di consentire lo svolgimento delle mansioni lavorative

L'utilizzo della comunicazione tramite e-mail deve essere limitato esclusivamente agli scopi di servizio. È, pertanto, vietato utilizzare la casella di posta elettronica dell'AC per la trasmissione o ricezione di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.

Attraverso le caselle e-mail istituzionali gli utenti rappresentano pubblicamente l'Ente e, per questo motivo, viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque in modo tale da riflettere positivamente l'immagine dell'AC.

È obbligatorio controllare preliminarmente i file allegati nelle comunicazioni di posta elettronica. In particolare, si deve evitare, secondo le regole di buona diligenza, l'apertura e la lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità o che contengano link o allegati del tipo .exe, .com, .vbs, .htm, .scr, .bat, .js, .pif.

L'iscrizione a mailing-list o newsletter esterne con l'indirizzo ricevuto è concessa esclusivamente per motivi di servizio. Prima dell'iscrizione, l'utente è tenuto a impostare verificare anticipatamente l'affidabilità del sito che offre il servizio.

Non è consentito l'invio automatico di comunicazioni e-mail dalla casella di posta istituzionale a caselle private del dipendente

(attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.).

In questa ultima ipotesi, l'utente è tenuto a impostare un messaggio "Out of Office" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando, quale recapito temporaneo, la casella e-mail dell'Ente (**corrispondenza@aciroma.it**).

È vietato l'invio di messaggi di posta elettronica in nome e per conto di un altro utente.

Nell'utilizzo della posta elettronica, l'utente deve:

- conservare la password con la massima riservatezza e diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti, evitando di utilizzare l'account di posta come "archivio" di file;
- prestare attenzione alla dimensione degli allegati, curando di aprire gli stessi solo dopo aver attentamente verificato l'attendibilità dei mittenti, in particolare se sconosciuti;
- accertarsi con cura 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 mittenti conosciuti e cancellare preventivamente le altre, avendo cura di verificare l'effettiva riconducibilità del nome pubblico del mittente ad una casella di posta istituzionale;

È vietato utilizzare impropriamente la posta elettronica, ad esempio per la diffusione di messaggi diffamatori, osceni, di profanazione, lettere minatorie o di offesa razziale, messaggi commerciali o di propaganda, "catene di S. Antonio" nonché l'utilizzo della posta elettronica con modalità di forum;

Il personale, nelle comunicazioni a mezzo posta elettronica, deve rispettare, di norma, gli ordinari riporti amministrativi; in ogni caso, ciascun dipendente è tenuto ad utilizzare un linguaggio appropriato ed una forma espositiva adeguata, secondo il comune sentire.

L'invio di messaggi di posta elettronica a un elevato numero di destinatari è consentito solo qualora richiesto da specifiche esigenze di lavoro; è fatto salvo, in ogni caso, l'invio di circolari o analoghi messaggi.

Nell'utilizzo sulla posta elettronica si applicano le ordinarie regole di riservatezza e di segreto per ragioni d'ufficio; i documenti di lavoro possono essere inviati ad indirizzi di posta elettronica esterni solo se necessario per l'attività lavorativa.

Tramite posta elettronica possono essere inviati file allegati, le cui dimensioni devono essere commisurate alla capacità delle infrastrutture adottate al fine di non causare l'indisponibilità dei sistemi.

Il personale è tenuto a non dare seguito a messaggi con dubbi oggetti e provenienza in cui vengano richieste informazioni riguardanti dati personali e/o credenziali di autenticazione.

15.2 – *Delega a "fiduciario"*

Ciascun dipendente può delegare un altro dipendente quale "fiduciario", al fine di verificare i contenuti dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate alla attività lavorativa; il "fiduciario" è autorizzato ad inoltrare al Direttore o ad altro dipendente dallo stesso autorizzato, i messaggi ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

In caso di contemporanea assenza del dipendente delegante e del "fiduciario", ovvero nel caso in cui non sia stata rilasciata alcuna delega, e sussistendo urgenza e comprovata necessità, la casella di posta elettronica può essere visionata dal Direttore; di tale eventualità deve essere data informativa al predetto dipendente.

Art. 16 - Posta elettronica ordinaria condivisa e Posta elettronica certificata

Per le esigenze di servizio l'Ente mantiene attiva la casella di posta elettronica ordinaria **corrispondenza@aciroma.it**, la cui gestione, consultazione e utilizzo è condiviso da più dipendenti.

Analogamente l'Ente mantiene attive caselle di Posta Elettronica Certificata (PEC) dedicate alle comunicazioni istituzionali, secondo quanto previsto nel Manuale di gestione documentale.

Ferma restando l'applicazione delle prescrizioni di cui all'articolo precedente, l'AC stabilisce le seguenti ulteriori misure finalizzate ad un corretto utilizzo della posta elettronica condivisa e della PEC:

- il dipendente che risponde alle richieste avanzate attraverso le caselle di posta condivise dovrà apporre in calce alle stesse il proprio nome e cognome, al fine di garantire la massima trasparenza;
- le risposte fornite tramite le caselle di posta elettronica condivise possono essere consultate da ciascun dipendente che ne abbia l'accesso;
- le risposte fornite sono archiviate con le stesse modalità e gli stessi tempi previsti per le caselle di posta elettronica istituzionale personale.

I livelli di abilitazione per la consultazione e l'utilizzo della PEC son stabiliti nelle regole di sicurezza per il Protocollo Elettronico, con cui la casella di PEC è connessa.

16.1 - *Cessazione dell'indirizzo di Posta Elettronica Aziendale*

In caso di cessazione del rapporto di lavoro, l'utente è tenuto ad eliminare i messaggi di posta elettronica il cui contenuto non ritenga utile per assicurare la continuità funzionale delle attività svolte.

L'indirizzo di posta elettronica verrà disabilitato dall'Ente entro 30

giorni.

In ogni caso, l'Ente si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie attività.

16.2 - *Controlli sull'utilizzo di Internet e della posta elettronica*

L'AC adotta idonei strumenti di controllo graduato e iniziative formative, al fine di indirizzare i dipendenti verso un uso corretto e pertinente della posta elettronica e di Internet.

L'Ente può attivare forme di controllo anonimo, preliminarmente su dati aggregati, riferiti a specifiche aree lavorative o strutture organizzative.

A fronte di un rilevato utilizzo anomalo, il controllo può concludersi con un avviso generalizzato avente come scopo quello di invitare i dipendenti ad attenersi scrupolosamente alle istruzioni impartite circa l'utilizzo degli strumenti di lavoro.

In caso di successivi ripetuti utilizzi anomali dei sistemi e delle dotazioni informatiche, potranno essere effettuati controlli individuali sui dipendenti previa informativa ai soggetti sindacali.

Art. 17 – Formazione e sensibilizzazione

L'Ente promuove periodiche attività di formazione e sensibilizzazione degli utenti su tematiche relative alla sicurezza informatica, alla protezione dei dati personali, al rischio di attacchi informatici e all'uso corretto delle risorse digitali.

Le attività possono avvenire mediante incontri formativi, avvisi interni, linee guida operative o moduli e-learning.

Capo V — PROCEDURA PER VIOLAZIONI DEI DATI PERSONALI E PER L'ESERCIZIO DELLE RICHIESTE DI ESERCIZIO DEI DIRITTI

Art. 18 – Rinvio

Le procedure per la gestione delle violazioni di dati personali (data breach) e delle richieste di esercizio dei diritti formulate dagli interessati sono disciplinate nel Regolamento Privacy dell'Automobile Club Roma.

Capo VI — SANZIONI, COMUNICAZIONI, APPROVAZIONE

Art. 19 – Sanzioni

Il mancato rispetto o la violazione delle regole contenute nel presente documento è perseguibile con le sanzioni disciplinari previste dalla contrattazione collettiva, nonché con le eventuali azioni civili, penali e amministrativo-contabili.

In caso di violazione accertata delle regole e degli obblighi previsti nel presente documento, 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 dati e degli strumenti informatici.

Art. 20 – Informativa agli utenti ex art. 13 Regolamento (UE) 2016/679

Le disposizioni del presente documento che comportano il trattamento di dati personali valgono quale informativa agli utenti e ai dipendenti ai sensi dell'art. 13 del Regolamento (UE) 2016/679.