REGOLAMENTO
IN TEMA DI UTILIZZO E CONTROLLO
DEGLI STRUMENTI
ELETTRONICI, INFORMATICI E TECNOLOGICI

Aggiornamento settembre 2021

Approvato con deliberazione del Consiglio di Amministrazione n. 120 del 30/09/2021

Premessa

Il presente Regolamento intende fornire ai dipendenti, collaboratori, nonché a chiunque abbia accesso autorizzato agli strumenti informatici del Consorzio (di seguito anche denominati "incaricati"), le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.
Ogni utente è tenuto a rispettare il Regolamento, che è reso disponibile tramite le modalità specificate al successivo art. 9.

Art. 1) - Soggetti che possono utilizzare strumenti elettronici, informatici e tecnologici

1. L'utilizzo degli strumenti tecnologici assegnati in dotazione (computer, telefoni, modem, tablet o altro tipo di dispositivo elettronico, comprese chiavette usb, hard disk, smart card o altri sistemi di memorizzazione o di gestione dei dati ecc.) e l'accesso ad internet è accordato al dipendente con la lettera di designazione ad "incaricato" e con le relative istruzioni riguardanti anche la sicurezza dei dati.
   L'utilizzo è altresì accordato al collaboratore che abbia accesso alle dotazioni informatiche del Consorzio per necessità strettamente legate all'espletamento del proprio incarico, nonché a chiunque abbia accesso autorizzato agli strumenti informatici del Consorzio
2. Il datore di lavoro potrà designare uno o più "responsabili", fornendo loro precise istruzioni sui tipi di controllo ammessi e sulle relative modalità.
3. Agli incaricati alla manutenzione è vietato l'accesso a dati personali presenti in cartelle o spazi di memoria eventualmente assegnati ai dipendenti ed è posto l'obbligo di svolgere solo le operazioni strettamente necessarie per adempiere al loro incarico, con divieto di realizzare attività di controllo a distanza, soprattutto di propria iniziativa; ai dipendenti sono resi noti i nominativi ed i compiti dei manutentori.
4. L'amministratore di sistema può compiere le operazioni strettamente necessarie per adempiere al suo incarico.

Art. 2) Divieti di utilizzo

1. Al fine di garantire la funzionalità, la sicurezza ed il corretto impiego degli strumenti elettronici e, al tempo stesso, la protezione della riservatezza dei dipendenti, messa a rischio dalla possibilità di costante monitoraggio offerte dalla tecnologia (es.: profilazioni, comunicazione/diffusione di dati personali, anche particolari ex art. 9-10 del Regolamento 679/2016), è vietato rispetto all'utilizzo del computer:
   - l'utilizzo del sistema informatico del Consorzio per motivi non lavorativi o non di servizio;
   - l'installazione di programmi ulteriori rispetto a quelli forniti dal Consorzio;
   - la modificazione delle configurazioni impostate
   - aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani
   - ostacolare l'azione dell'antivirus.

2. Rispetto all'utilizzo di internet, in particolare, i divieti riguardano:
   - la navigazione su siti non correlati con la prestazione lavorativa;
   - il download di programmi o di file, non correlati con la prestazione lavorativa salvo espressa autorizzazione da parte del Consorzio;
   - la partecipazione a forum, non preventivamente autorizzata e l'utilizzo di chat line, partecipazione ad aste on-line (es.: e-bay);

- l'attività di trading online;
- la conservazione di file a contenuto offensivo, discriminatorio, illecito penalmente e civilmente;
- l'uso per finalità ludiche;
- l'uso di strumenti di comunicazione non attinenti all'attività lavorativa
- utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248 e s.m.i.). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, …) se non espressamente autorizzato dal Consorzio.

3. Rispetto all'utilizzo della posta elettronica, i divieti riguardano:
    - l'uso della posta elettronica per ragioni non attinenti ai compiti affidati;
    - l'invio o la memorizzazione di messaggi offensivi o discriminatori;
    - l'uso della posta elettronica per documenti classificati come riservati o confidenziali;
    - l'uso per partecipare a dibattiti, forum o mail list di contenuto offensivo o discriminatorio;
    - la costituzione di cartelle segrete, nascoste o criptate;
    - l'uso della posta elettronica per la registrazione a servizi non aziendali o per la registrazione ad account non aziendali (gmail, google drive, dropbox, ecc.).

4. Rispetto all'utilizzo dei telefoni, smartphone, tablet, fax, fotocopiatrici aziendali, si stabilisce quanto segue:
    - È consentito l'uso esclusivamente per lo svolgimento dell'attività lavorativa;
    - L'assegnatario è custode e responsabile del bene aziendale;
    - È vietata l'installazione di app non autorizzate e l'utilizzo della fotocamera per motivi personali e la configurazione di account personali;
    - L'eventuale uso promiscuo del telefono aziendale è possibile in presenza di preventiva autorizzazione scritta e in conformità alle istruzioni che verranno impartite.

Art. 3) Prevenzione all'utilizzo improprio

1. Al fine di prevenire l'utilizzo improprio degli strumenti informatici non è tollerato, relativamente ad internet ed alla posta elettronica, l'uso privato.
2. ogni incaricato del trattamento è tenuto a garantire e conservare la riservatezza e la segretezza dei dati personali di cui ha conoscenza e ad usarli esclusivamente per finalità congruenti con la base giuridica che ne autorizza il trattamento.
3. In caso di intervento tecnico da parte degli AdS (Amministratori di Sistema), per il ripristino di dati accidentalmente cancellati e per il ripristino della funzionalità e delle impostazioni della posta elettronica questi, limitatamente alle necessità proprie dell'intervento, possono visualizzare l'indirizzo e l'oggetto delle mail.
4. E' consentito ai dipendenti avvalersi di funzionalità automatiche del sistema in caso di assenze programmate (ferie, lavoro fuori sede, etc.), al fine di consentire o l'invio automatico di messaggi di risposta contenenti le "coordinate" (elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto del Consorzio.
5. In caso di assenza improvvisa o prolungata del dipendente, se improrogabili necessità di lavoro richiedano la conoscenza dei messaggi di posta elettronica, l'interessato può delegare un altro lavoratore (fiduciario); il delegato riferirà al datore di lavoro i "dati rilevanti" per lo svolgimento dell'attività lavorativa; il datore di lavoro ne darà comunicazione all'interessato. Nel caso si verificasse la necessità di visualizzare per motivi di servizio il pc del lavoratore assente in

concomitante assenza del lavoratore indicato come fiduciario il datore di lavoro potrà accedere al pc direttamente o tramite un proprio incaricato utilizzando le credenziali depositate presso il custode delle credenziali. L'evento dovrà essere reso noto al lavoratore che alla ripresa del lavoro dovrà provvedere alla sostituzione delle password.

6. L'e-mail contenente i nomi degli ex dipendenti (licenziati, dimessisi) andrà "chiusa"; nel caso in cui però il titolare, per non perdere comunicazioni aziendali, intenda comunicare a terzi tale chiusura dovrà segnalare un account aziendale alternativo rispetto al contatto precedentemente utilizzato.
7. Alla dismissione di un dipendente dall'attività CON.AMI si dovrà procedere a:
    - Inserimento di un messaggio di risposta automatico per la comunicazione agli utenti che scrivono al dipendente per il quale è cessato il rapporto di lavoro, a far data dal momento di cessazione del contratto stesso;
    - Creazione di un archivio pst della relativa posta elettronica e dei file dal dipendente/ coloro che abbiano avuto accesso autorizzato agli strumenti informatici del Consorzio)];elaborati/modificati su rete, entro 60 giorni naturali consecutivi dal momento di cessazione del contratto stesso;
    - Inserimento in rete di una cartella inerente il dipendente/incaricato del trattamento per il quale è cessato il contratto di lavoro/rapporto, alla quale un dipendente all'uopo nominato potrà accedere per proprie esigenze di servizio o anche su richiesta di terzi, per la ricerca/controllo dell'avanzamento di talune attività che interessavano il dipendente/incaricato del trattamento in questione;
7. Cancellazione dell'utente dal Dominio Utenti CON.AMI entro 60 giorni naturali consecutivi dal momento di cessazione del contratto stesso. L'uso della posta elettronica deve rispettare i seguenti principi:
    1. Tutela dell'immagine del consorzio;
    2. Rispetto dell'etica aziendale espressa nell'ambito del MOG 231;
    3. Osservanza della riservatezza da parte dei lavoratori;
    4. Correttezza nei rapporti tra colleghi;
    5. Impiego di un linguaggio appropriato;
    6. Uso succinto dello strumento (scrivere e allegare lo stretto necessario);
    7. Rispetto delle normative vigenti.

La veicolazione per posta elettronica di informazioni che possano "impegnare" il consorzio deve essere autorizzata preventivamente.

Non si possono inviare informazioni confidenziali, critiche, riservate senza autorizzazione, più in generale, non è consentito inoltrare a utenti esterni mail di corrispondenza interna aziendali.

Nel caso in cui ci si accorga di aver sbagliato il destinatario del messaggio contenente dati del consorzio, si dovrà procedere con l'immediata richiesta al destinatario di cancellare l'e-mail ricevuta per errore e con la comunicazione dell'avvenuto al titolare del trattamento.

Art. 4) Gestione password

1. Ogni lavoratore è munito di un nome Utente e Password che lo abilitano ad utilizzare il PC presente nella postazione aziendale e a collegarsi al wi-fi aziendale.
2. La Password è strettamente personale, deve essere costituita da un minimo di 8 caratteri alfanumerici che non contengano riferimenti personali all'incaricato.
3. Ogni lavoratore dovrà modificare la Password almeno ogni sei mesi. Una volta modificata la password, il titolare della stessa dovrà compilare il "modulo password incaricato" in suo possesso, chiudere il modulo in una busta che dovrà essere consegnata al custode delle credenziali indicato come depositario delle stesse presso l'ufficio Segreteria.

Art. 5) Possibilità di controlli e loro gradualità

1. Verranno effettuati controlli sul server volti ad individuare in forma cumulativa l'accesso alla rete e ai siti visitati soprattutto nelle circostanze in cui si verificassero flussi anomali di dati. Nel caso in cui da queste verifiche emergesse un uso in contrasto con la linea del presente regolamento la direzione aziendale valuterà modalità diverse delle attività di controllo.
2. In linea generale, il diritto del datore di lavoro di effettuare controlli identificativi del lavoratore, sussiste quando ciò sia dettato da:
    - esigenze per l'esercizio o la difesa in sede giudiziaria;
    - riscontri di gravi inadempienze della prestazione lavorativa o comunque di attività idonee a compromettere il vincolo fiduciario con il datore di lavoro;
    - oggettivi indizi di commissione del reato;
    - esigenze di salvaguardia della vita o dell'incolumità di terzi;
    - norme specifiche di legge o dall'autorità giudiziaria.
3. Le esigenze organizzative, produttive, di sicurezza ed il mancato rispetto del presente regolamento che possa evidenziare comportamenti anomali (evento dannoso, situazione di pericolo, rischi di responsabilità per il Consorzio, interferenze, rischio o danno per altri dipendenti), legittimano il datore di lavoro al controllo sull'utilizzo del web e dell'e-mail.
4. Potrebbero intervenire da parte del Datore di Lavoro, controlli delle comunicazioni private in circostanze legate alle esigenze di sicurezza del sistema; per esigenze difensive nel caso in cui il datore di lavoro sia responsabile per le azioni del lavoratore o vittima delle sue condotte; per il rilevamento della presenza di virus informatici ed altri situazioni similari. Il datore di lavoro deve considerarsi legittimato ad effettuare controlli *ex post* (eseguiti a posteriore) legati alla posta elettronica ed alla navigazione su Internet del lavoratore, per finalità di carattere difensivo (volti ad accertare le condotte illecite dei lavoratori) cioè, per soddisfare esigenze legate all'accertamento di un illecito penale e/o disciplinare.
5. Relativamente ai dati rinvenibili mediante impiego del sistema di videosorveglianza, adottato dalla società per finalità unicamente di prevenzione e salvaguardia dell'immobile aziendale, gli stessi saranno trattati nell'ambito della finalità sopra indicata.

Art. 6) Conservazione sui dati

1. Sono memorizzate temporaneamente le informazioni relative all'uso degli strumenti informatici ed elettronici indispensabili per le seguenti finalità:
    - protezione dell'intera rete da e verso l'esterno (firewall);
    - più efficiente utilizzo del collegamento Internet (proxy server);
    - difesa della corrispondenza e navigazione informatica (antispamming/antivirus);
    - controllo automatico del contenuto dei siti (web filtering).
2. I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati relativi agli accessi ad Internet e al traffico telematico. Eccezionalmente la conservazione può essere protratta, per il tempo indispensabile e per le sole informazioni necessarie, in relazione:
    - all'indispensabilità dei dati rispetto all'esercizio o difesa di un diritto in sede giudiziaria;
    - all'obbligo di custodire o consegnare i dati per specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Ogni strumento informatico o tecnologico affidato agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti al Consorzio che provvederà a distruggerli o a ricondizionarli seguendo le

norme di legge in vigore al momento. In particolare il Consorzio provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati in quanto non più necessari.

Art. 7) Sanzioni

1. La mancata osservanza delle disposizioni comporterà l'applicazione delle sanzioni previste dal vigente contratto collettivo di lavoro applicato dal Consorzio e/o dal codice sanzionatorio adottato nell'ambito del Modello 231.
2. E' richiamata l'attenzione dei lavoratori sul fatto che l'uso improprio degli strumenti aziendali può anche integrare le seguenti ipotesi di reato:
   - furto;
   - turbato funzionamento di sistemi informatici;
   - accesso abusivo a sistemi informatici/telematici;
   - diffusione di programmi diretti a danneggiare o interrompere un sistema informatico;
   - violazione, sottrazione e soppressione di corrispondenza;
   - intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
   - installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche/telematiche;
   - danneggiamento di sistemi informatici/telematici;
   - frode informatica.

Art. 8) Esercizio dei diritti del dipendente/incaricati

1. I diritti di cui all'art. 15 del GDPR n. 679/2016 vanno esercitati rivolgendosi al soggetto indicato nell'informativa resa dal Titolare del Trattamento Dati. Il Titolare si riserva la facoltà di proporre altro soggetto o unità operativa, previa informativa ai dipendenti/incaricati.

Art. 9) Pubblicazione del Regolamento

1. Il presente Regolamento:
   - viene pubblicato sul sito del Consorzio – www.con.ami.it- nella sezione "Amministrazione Trasparente";
   - verrà divulgato a tutti i dipendenti.

Art. 10) Informativa

1. Ai sensi degli artt. 13 e ss. GDPR n. 679/2016, fermo e richiamato quanto riportato sul sito internet del consorzio, si comunica che:
   - l'Amministratore di sistema, può effettuare il trattamento dei dati relativi al traffico sulla rete;
   - il titolare dei dati di traffico è il Direttore Generale;
   - la presa visione e l'accettazione delle condizioni contenute nel presente regolamento costituiscono l'informativa e l'esplicito consenso da parte dell'utente alla raccolta ed all'eventuale trattamento dei dati relativi al traffico.

Art. 11) Entrata in vigore del regolamento

Il nuovo regolamento entra in vigore a partire dalla data di approvazione dello stesso da parte del Consiglio di Amministrazione.

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.