# REGOLAMENTO IN TEMA DI UTILIZZO E CONTROLLO DEGLI STRUMENTI ELETTRONICI

## Art. 1) - Soggetti che possono utilizzare strumenti elettronici

1. L'utilizzo della posta elettronica 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.
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, anche 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 sensibili), 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 personali ulteriori rispetto a quelli forniti dal Consorzio;
    - la modificazione delle configurazioni impostate.

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

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 riservati o confidenziali;
    - l'uso per partecipare a dibattiti, forum o mail list di contenuto offensivo o discriminatorio;

- la costituzione di cartelle segrete.

**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. 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 delle posta elettronica questi, limitatamente alle necessità proprie dell'intervento, possono visualizzare l'indirizzo e l'oggetto delle mail.
3. 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.
4. 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.
5. 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.

**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.
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. Il 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;
   - 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.

**Art. 6) Conservazione sui dati**

1. Sono memorizzate temporaneamente le informazioni relative all'uso degli strumenti 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 dei 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.

**Art. 7) Sanzioni**

1. La mancata osservanza delle disposizioni comporterà l'applicazione delle sanzioni previste dal vigente contratto collettivo di lavoro applicato dal Consorzio.
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 di energie;
   - 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**

1. I diritti di cui all'art. 7 del Codice della privacy vanno esercitati rivolgendosi al soggetto indicato nell'informativa del datore di lavoro. Il datore di lavoro si riserva la facoltà di proporre altro soggetto o unità operativa, previa informativa ai dipendenti.

**Art. 9) Pubblicazione del Regolamento**

1. Il presente Regolamento:
   - viene pubblicato sul sito del Consorzio – www.con.ami.it- nella sezione "Amministrazione Trasparente";
   - viene diffuso in occasione di un evento formativo a tutti i dipendenti in materia di privacy.

**Art. 10) Informativa**

1. Ai sensi dell'art. 13 del D.Lgs. n. 196 del 30 giugno 2003 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) Presa visione ed accettazione del Regolamento**

| Nome e Cognome del lavoratore | Firma per ricevuta del presente Regolamento |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |