

ISTITUTO CESANA-MALANOTTI VITTORIO VENETO

Regolamento per l'utilizzo dei sistemi informatici presso le strutture e servizi gestiti dall'Istituto Cesana Malanotti.

(Approvato con Decreto del Segretario Direttore - Area segreteria n. 1 del 31.3.2017 – in vigore dal 2.05.2017)

Indice

1. Entrata in vigore del regolamento e pubblicità
2. Campo di applicazione del regolamento
3. Utilizzo del Personal Computer
4. Gestione ed assegnazione delle credenziali di autenticazione
5. Utilizzo della rete dell'Istituto Cesana Malanotti
6. Utilizzo e conservazione dei supporti rimovibili
7. Utilizzo di PC portatili
8. Uso della posta elettronica
9. Navigazione in Internet
10. Protezione antivirus
11. Utilizzo dei telefoni, fax e fotocopiatrici aziendali
12. Osservanza delle disposizioni in materia di Privacy
13. Accesso ai dati trattati dall'utente
14. Sistema di controlli gradualì
15. Sanzioni
16. Aggiornamento e revisione

Premessa:

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'Istituto Cesana Malanotti e gli utenti (dipendenti e collaboratori dello stesso) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Ente stesso.

Premesso quindi che **l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro**, l'Istituto Cesana Malanotti ha adottato un regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D.Lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Considerato inoltre che l'Istituto Cesana Malanotti nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

1. Entrata in vigore del regolamento e pubblicità

1.1 Il presente regolamento entra in vigore il 02/05/2017. 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.

1.2 Copia del regolamento, oltre ad essere affisso all'albo dell'Ente e nel sito istituzionale, verrà consegnato a ciascun dipendente interessato.

2. Campo di applicazione del regolamento

2.1 Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.).

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento". Eventuali deroghe al presente regolamento potranno essere disposte dal Segretario direttore.

3. Utilizzo del Personal Computer

3.1 Il **Personal Computer** affidato all'utente è uno strumento di lavoro. **Ogni utilizzo non inerente all'attività lavorativa è vietato** perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'Istituto Cesana Malanotti solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente regolamento.

3.3 L'Istituto Cesana Malanotti rende noto che il Direttore Amministrativo è il responsabile del servizio informatico ed è stato incaricato delle funzioni di Amministratore di sistema. In quanto tale, esso è autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 8.2 e 9.1, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Istituto Cesana Malanotti, si applica anche in caso di assenza prolungata od impedimento dell'utente.

3.4 L'Amministratore di sistema ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, ecc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico

e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

3.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente previsti né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'Istituto Cesana Malanotti a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

3.6 Salvo preventiva espressa autorizzazione del Amministratore di sistema non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...).

3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 10 del presente regolamento relativo alle procedure di protezione antivirus.

3.8 Il **Personal Computer deve essere spento ogni sera prima di lasciare l'ufficio o il servizio**. Le postazioni utilizzate nei servizi attivi 24 ore, possono essere tenute in funzione durante i periodi di effettivo utilizzo, anche se intervallati da brevi pause, sarà cura dell'utente provvedere allo spegnimento in previsione di pause prolungate (es. 1 h). In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

4. Gestione ed assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dall'Amministratore di sistema o suo delegato, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dall'Amministratore di sistema, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'Amministratore di sistema.

4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

4.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (ogni tre mesi nel caso di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

4.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con l'Amministratore di sistema.

4.6 Soggetto preposto alla custodia delle credenziali di autenticazione è l'Amministratore di sistema o un suo delegato.

5. Utilizzo della rete dell'Istituto Cesana Malanotti.

5.1 Per l'accesso alla rete dell'Istituto Cesana Malanotti ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

5.2 **È proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato.** Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

5.3 Le cartelle utenti presenti nei server dell'Istituto Cesana Malanotti sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. **Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.** Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte della Direzione tramite l'Amministratore di sistema. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato dalla Direzione. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

5.4 L'Amministratore di sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

5.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti

necessario evitare un'archiviazione ridondante.

6. Utilizzo e conservazione dei supporti rimovibili

6.1 Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

6.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare l'Amministratore di sistema e seguire le istruzioni da questo impartite.

6.3 In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

6.4 E' vietato l'utilizzo di supporti rimovibili personali.

6.5 L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

7. Utilizzo di PC portatili

7.1 L'utente è responsabile del PC portatile assegnatogli dalla Direzione e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

7.2 Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

7.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

7.4 Tali disposizioni si applicano anche nei confronti di incaricati esterni.

8. Uso della posta elettronica

8.1 La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica@cesnamalanotti.it per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali

(es.mp3) non legati all'attività lavorativa;

- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;

- la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore di sistema. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

8.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali dell'Istituto Cesana Malanotti ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile d'ufficio o di area.

8.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, ...), devono essere autorizzate e firmate dalla Direzione e/o dai Responsabili d'ufficio, a seconda del loro contenuto e dei destinatari delle stesse.

8.6 È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

8.7 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella), invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. Tale funzionalità deve essere attivata dall'utente.

8.8 In caso di assenza non programmata (ad es. per malattia) la procedura, qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni, verrà attivata a cura dell'Istituto Cesana Malanotti.

8.9 Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'Ente, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 8.7, assenza non programmata ed impossibilità di attendere i due

giorni di cui al punto 8.8).

8.10 Nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la tempestività ed efficacia dell'intervento, l'Amministratore di sistema potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3.

8.11 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato della procedura potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy aziendale.

9. Navigazione in Internet

9.1 Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa. L'Amministrazione, tuttavia, ammette in via eccezionale che tale connessione venga utilizzata anche per scopi non immediatamente correlati alla prestazione lavorativa, purché ciò avvenga nel rispetto dei principi di ragionevolezza e di buona fede (imprescindibili nella esecuzione del rapporto di lavoro) e, comunque, non metta a repentaglio l'integrità e la riservatezza dei dati, delle informazioni e dell'intero sistema informatico dell'Amministrazione ovvero provochi per la stessa un danno economico. Ciò comporta che l'utente finale, fermo restando il rispetto delle disposizioni di legge in materia, del CCNL, degli obblighi di riservatezza e degli standard previsti da specifiche normative interne, non può utilizzare l'accesso a internet, per motivi personali, se non in maniera breve ed occasionale e, comunque, con modalità che non arrechino intralcio/rallentamento alla normale attività lavorativa propria e di terzi. Tale eccezionalità è in ogni caso soggetta ad autorizzazione del Responsabile di ufficio o area.

9.2 In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato l'Amministratore di sistema);

- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, dovranno essere effettuate esclusivamente a norma delle vigenti disposizioni di legge in materia e relativi regolamenti applicativi vigenti nell'ICM;

- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;

- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;

- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Istituto Cesana Malanotti rende peraltro nota l'intenzione di adottare uno specifico sistema di blocco o filtro automatico che prevenga determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.

9.4 Gli eventuali controlli, compiuti dall'Amministratore di sistema ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 3 mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

10. Protezione antivirus

10.1 Il sistema informatico dell'Istituto Cesana Malanotti è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto all'Amministratore di sistema o suo delegato.

10.3 Ogni dispositivo magnetico di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato all'Amministratore di sistema o suo delegato.

11. Utilizzo dei telefoni, fax e fotocopiatrici aziendali

11.1 Il telefono aziendale affidato all'utente è uno strumento di lavoro. **Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.** La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza ed a seguito autorizzazione del Responsabile dell'Ufficio e/o servizio.

11.2 Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. **Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.**

11.3 È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

11.4 È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile dell'ufficio o servizio.

12. Osservanza delle disposizioni in materia di Privacy

12.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Disciplinare tecnico allegato al D.Lgs. n. 196/2003.

13. Accesso ai dati trattati dall'utente

13.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione, tramite l'Amministratore di sistema o suo delegato o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

14. Sistemi di controlli graduali

14.1 In caso di anomalie, l'Amministratore di sistema o suo delegato

effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

14.2 In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

15. Sanzioni

15.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL Area Dirigenza e personale non dirigente Enti Locali, nonché con tutte le azioni civili e penali previste anche in termini di violazione dei doveri del pubblico dipendente.

16. Aggiornamento e revisione

16.1 Il presente regolamento verrà aggiornato sistematicamente a norma delle vigenti disposizioni. Da tale data sono da ritenersi abrogate tutte le precedenti disposizioni e/o direttive.

Data 31.03.2017

Il Segretario Direttore
Dott. Pasquale Bongiorno