Camera di Commercio
Ravenna

Allegato B) alla Delib. n. 11 del verbale di Giunta del 27.1.2014

Codice di comportamento integrato dei dipendenti

della Camera di commercio di Ravenna

In attuazione all'art. 54 del D.Lgs. n. 165/2001

gennaio 2014

ART. 1 – PREMESSA

1. I principi e i contenuti del presente Codice di comportamento dei dipendenti della Camera di Commercio di Ravenna sono da intendersi quale ulteriore specificazione del Codice di comportamento dei dipendenti pubblici, adottato, ai sensi dell'art. 54 del D.Lgs. n. 165/2001, con Decreto del Presidente della Repubblica n. 62 del 16 aprile 2013, il cui contenuto deve considerarsi base minima e indefettibile e, pertanto, integralmente richiamato.

2. I principi e i contenuti del presente Codice costituiscono esemplificazione degli obblighi di diligenza, lealtà e imparzialità che qualificano il corretto adempimento della prestazione lavorativa e pertanto la loro inosservanza implica nei confronti del dipendente l'insorgenza di responsabilità disciplinare.

3. Il Segretario Generale è Responsabile della prevenzione della corruzione nell'Ente e concorre alla definizione di misure idonee a prevenire e contrastare i fenomeni di corruzione e a controllarne il rispetto da parte dei dipendenti.

ART. 2 – AMBITO DI APPLICAZIONE

1. Il presente codice si applica ai dipendenti della Camera di Commercio di Ravenna il cui rapporto di lavoro è disciplinato in base all'articolo 2, commi 2 e 3, del decreto legislativo 30 marzo 2001, n. 165.

2. La Camera di Commercio di Ravenna estende, per quanto compatibili, gli obblighi di condotta previsti dal presente codice ai titolari di organi, ai dipendenti dell' Azienda speciale, a tutti i collaboratori o consulenti, con qualsiasi tipologia di contratto o incarico ed a qualsiasi titolo, ai collaboratori a qualsiasi titolo di imprese fornitrici di beni o servizi che realizzano opere in favore dell'amministrazione. A tale fine, negli atti di incarico o nei contratti di acquisizioni delle collaborazioni, delle consulenze o dei servizi, devono essere inserite apposite disposizioni o clausole di risoluzione o decadenza del rapporto in caso di violazione degli obblighi derivanti dal presente codice.

ART. 3 – PRINCIPI GENERALI

1. Il dipendente della Camera di Commercio di Ravenna conforma la sua condotta ai principi di buon andamento e imparzialità dell'amministrazione. Egli assicura il rispetto della legge e persegue esclusivamente l'interesse pubblico che gli è affidato, costituito dalla promozione degli interessi generali e lo sviluppo del mercato.

2. Il dipendente ispira la propria azione ai principi di qualità e trasparenza, efficacia, economicità ed efficienza, favorendo la partecipazione dell'utenza.

3. Il dipendente mantiene una posizione di indipendenza al fine di evitare di prendere decisioni o svolgere attività in situazioni, anche solo apparenti, di conflitto di interessi.

ART. 4 – INCOMPATIBILITA'

1. Il dipendente della Camera di Commercio di Ravenna non svolge alcuna attività che contrasti con il corretto adempimento dei compiti d'ufficio e si impegna ad evitare situazioni e comportamenti che possano nuocere agli interessi e all'immagine dell'Amministrazione.

2. Fermo restando le disposizioni di cui all'art. 53 D.Lgs. n. 165/2001, i dipendenti della Camera di Commercio di Ravenna non possono svolgere incarichi retribuiti che non siano stati conferiti o previamente autorizzati dall'amministrazione di appartenenza.

3. Le autorizzazioni allo svolgimento di incarichi da parte dei dipendenti vanno richieste al Segretario Generale. Nella domanda il dipendente esplicita la tipologia dell'incarico, il soggetto conferente, la data di inizio e fine incarico, nonché l'importo del compenso, anche presunto.

4. Le autorizzazioni allo svolgimento di incarichi da parte dei dipendenti della Camera di Commercio vengono rilasciate dal Segretario Generale.

ART. 5 – REGALI, COMPENSI E ALTRE UTILITA'

1. Il dipendente della Camera di Commercio di Ravenna non chiede, per sé e per altri, né accetta regali o altre utilità, anche sotto forma di sconto, salvo quelli d'uso di modico valore effettuati occasionalmente nell'ambito delle normali relazioni di cortesia. Per regali di modico valore si intendono quelli di valore non superiore a € 150. In presenza di più regali nel corso dell'anno solare il limite complessivo da parte dello stesso soggetto non potrà comunque eccedere € 150. In questo caso i dipendenti hanno l'obbligo di comunicare all'Amministrazione i nomi di coloro che hanno disposto i regali o le altre utilità.

2. Il dipendente non offre, direttamente o indirettamente, regali o altre utilità a un proprio sovraordinato, ivi compresi quelli d'uso di modico valore.

3. Il dipendente non chiede né accetta, per sé e per altri, alcun regalo o altre utilità, comprese quelle di modico valore di cui al precedente comma, quando ciò costituisca corrispettivo per compiere o aver compiuto un atto del proprio ufficio, o in ogni caso da soggetti che possano trarre beneficio da attività, decisioni o atti compiuti dall'ufficio.

4. I regali e le altre utilità di valore superiore a € 150 comunque ricevuti devono essere messi a disposizione dell'Amministrazione che le utilizzerà per fini istituzionali.

5. Non sono ricompresi nella fattispecie di cui ai commi precedenti, e sono quindi ammessi, i gadget promozionali di modico valore, distribuiti genericamente all'Ente da fornitori/ditte appaltatrici.

6. Al fine di preservare il prestigio e l'imparzialità dell'Amministrazione, il Responsabile della prevenzione della corruzione vigila sulla corretta applicazione del presente articolo.

ART. 6 – OBBLIGO DI ASTENSIONE

1. I dipendenti della Camera di Commercio di Ravenna hanno l'obbligo di astenersi dal partecipare all'adozione di decisioni o attività (quali, a titolo meramente esemplificativo, la partecipazione a commissioni per la selezione del personale, per i bandi di gara, nonché per l'attribuzione di sovvenzioni comunque denominate) ogniqualvolta possano essere coinvolti interessi propri, ovvero di parenti, affini entro il secondo grado nonché persone con le quali abbiano rapporti di amicizia o frequentazione abituale.

2. Le comunicazioni di astensione, debitamente motivate, debbono essere inoltrate in forma scritta al dirigente dell'Area di appartenenza per la valutazione della sussistenza o meno dell'obbligo di astensione.

3. Sull'astensione del dipendente decide il dirigente dell'Area di appartenenza, il quale ne dà riscontro al Segretario Generale in qualità di Responsabile per la prevenzione della corruzione e cura la tenuta e l'archiviazione di tutte le decisioni di astensione dal medesimo adottate.

ART. 6 BIS – DISPOSIZIONI PER IL PERSONALE INCARICATO DI PROCEDURE DI ACQUISIZION BENI, SERVIZI E LAVORI

1. I dipendenti addetti all'ufficio Provveditorato o comunque incaricati di espletare le procedure di acquisizione di beni, servizi e lavori non conlcudono per conto dell'Ente contratti di appalto, fornitura, servizio, finanziamento o assicurazione con imprese con le quali abbiano stipulato contratti a titolo privato e dalle quali abbiano ricevuto altre utilità nel biennio precedente. Nei casi ivi previsti il dipendente interessato si astiene dal partecipare all'adozione delle decisioni e delle attività relative all'esecuzione del contratto, redigendo verbale scritto di tale astenzione.

2. Il dipendente che conclude accordi o negozi ovvero stipula contratti a titolo privato con persone fisiche o giuridiche con le quali abbia concluso, nel biennio precedente, uno dei contratti descritti al comma 1 per conto dell'Ente, ne informa per iscritto il proprio dirigente.

3. Il dipendente interessato, nei rapporti con i fornitori in argomento, adotta un comportamento trasparente, imparziale, obiettivo, integro e onesto, non influenzato da pressioni di qualsiasi tipo, né da interessi personali e finanziari.

4. Tale articolo si applica con riferimento alle transazioni private di importi superiori ad € 1.500,00.

ART. 6 TER – DISPOSIZIONI PER IL PERSONALE INCARICATO DI ACQUISIZIONE DI PERSONALE

1. I dipendenti, che nello svolgimento delle proprie funzioni, si occupano di procedure in materia di concorsi publici, devono dichiarare se sussistono situazioni di incompatibilità fra essi ed i candidati ai sensi degli artt. 51 e 52 del C.p.C.

2. Il dipendente non deve divulgare, volontariamente o per negligenza, informazioni inerenti la procedura selettiva al fine di avvantaggiare un partecipante, deve essere imparziale e contribuire al perseguimento dell'obiettivo dell'Ente, finalizzato a selezionare la persona più meritevole per competenze e capacità.

art. 6 QUATER – DISPOSIZIONI PER IL PERSONALE CON FUNZIONI DI CARATTERE ISPETTIVO

1. Il personale con funzioni di vigilanza e controllo sui prodotti e per la metrologia legale non può intrattenere rapporti commerciali stabili con le imprese destinatarie delle proprie attività.

2. Nel caso in cui per ragioni di comodità, vicinanza alla propria abitazione od altra causa, il medesimo personale abbia rapporti continui nel tempo con la stessa impresa od esercizio commerciale ovvero nel caso in cui sussistano rapporti di amicizia o parentela con i titolari delle imprese, deve prontamente comunicarlo al Responsabile; in tali casi il Responsabile assegna l'attività ad altri funzionari.

ART. 7 – COMUNICAZIONE DEGLI INTERESSI FINANZIARI E CONFLITTI D'INTERESSE

1. I dipendenti della Camera di Commercio di Ravenna comunicano la propria adesione o appartenenza ad associazioni, organizzazioni (esclusi i partiti politici e i sindacati), comitati i cui ambiti di interesse possono interferire con lo svolgimento delle attività dell'ufficio.

2. All'atto dell'assegnazione all'ufficio, i dipendenti comunicano per iscritto eventuali rapporti diretti e indiretti di collaborazione avuti con soggetti privati nei 3 anni precedenti e in qualunque modo retribuiti; hanno altresì l'obbligo di precisare se tali rapporti sussistono ancora, ovvero se sussistano con il coniuge, il convivente, i parenti e gli affini entro il secondo grado.

ART. 8 – PREVENZIONE DELLA CORRUZIONE

1. Il dipendente rispetta le misure necessarie alla prevenzione degli illeciti nell'Amministrazione e, in particolare, le prescrizioni contenute nel piano triennale di prevenzione della corruzione.

2. Ogni dipendente presta la sua collaborazione al Responsabile della prevenzione della corruzione, assicurando allo stesso ogni comunicazione di dati e informazioni richiesta e segnalando in via riservata allo stesso, oltre che al proprio dirigente, di propria iniziativa, eventuali situazioni di illecito nell'Amministrazione di cui sia venuto a conoscenza. Le segnalazioni da parte di un dirigente vengono indirizzate in via riservata al Segretario.

3. L'Amministrazione garantisce ogni misura di riservatezza a tutela del dipendente che segnala un illecito verificatosi nell'Amministrazione.

ART. 9 – TRASPARENZA E TRACCIABILITA'

1. Il dipendente assicura l'adempimento degli obblighi di trasparenza previsti secondo le disposizioni normative vigenti, prestando la massima collaborazione nell'elaborazione, reperimento e trasmissione dei dati sottoposti all'obbligo di pubblicazione sul sito istituzionale della Camera di Commercio.

2. La tracciabilità dei processi decisionali adottati dai dipendenti deve essere, in tutti i casi, garantita attraverso un adeguato supporto documentale, che consenta in ogni momento la replicabilità.

ART. 10 – VIGILANZA E MONITORAGGIO

Ai sensi dell'art. 54 del D.Lgs. n. 165/2001, i dirigenti di ogni area vigilano e monitorano sull'applicazione delle norme del Codice di Comportamento nazionale e quelle del presente documento, in collaborazione con l'Ufficio Procedimenti Disciplinari.

ART. 11 – OBBLIGHI DI COMPORTAMENTO

1. Il dipendente deve astenersi dallo spendere il nome e la qualifica camerale nei rapporti con terzi, ad esempio mediante interviste, stesura di articoli, partecipazione a convegni e/o seminari, ecc., se non preventivamente comunicato in forma scritta al dirigente dell'area di appartenenza.

2. Il dipendente non usa a fini privati le informazioni di cui dispone per ragioni d'ufficio.

3. Il dipendente cura il rispetto degli standard di qualità e di quantità fissati dall'Amministrazione ed opera al fine di assicurare la continuità del servizio.

4. Il dipendente in rapporto con il pubblico si fa riconoscere attraverso l'esposizione di badge o supporto identificativo; opera con spirito di servizio, correttezza, cortesia e disponibilità, nella maniera più completa ed accurata possibile.

5. Il dipendente adotta tutte le misure necessarie per garantire la sicurezza dei dati personali per i quali è incaricato del trattamento ovvero che riguardano la sua attività lavorativa. Effettua il trattamento secondo i principi di liceità e correttezza per la sola realizzazione delle

finalità cui sono destinati, rispetta le istruzioni impartite dal Responsabile, e mantiene la massima riservatezza, anche successivamente al termine dell'incarico medesimo, sui dati dei quali è venuto a conoscenza.

6. Il dipendente utilizza il materiale, le attrezzature, i servizi telefonici e telematici di cui dispone per ragioni d'ufficio nel rispetto dei vincoli posti dall'amministrazione; utilizza i mezzi di trasporto dell'Amministrazione – o in uso all'Amministrazione – posti a sua disposizione soltanto per lo svolgimento dei compiti d'ufficio, astenendosi dal trasportare terzi, se non per motivi d'ufficio.

ART. 12 – DISPOSIZIONI PARTICOLARI PER I DIRIGENTI

1. Ferma restando l'applicazione delle altre disposizioni del presente codice, le norme del presente articolo si applicano ai dirigenti.

2. Il dirigente, prima di assumere le sue funzioni, comunica all'Amministrazione e al responsabile della prevenzione della corruzione, le partecipazioni azionarie e gli altri interessi finanziari che possano porlo in conflitto di interessi con la funzione pubblica assegnatagli e dichiara se ha parenti e affini entro il secondo grado, coniuge o conviventi che esercitano attività politiche, professionali o economiche che li pongano in contatti frequenti con il sevizio che dovrà dirigere o che siano coinvolti nelle decisioni o nelle attività inerenti il servizio assegnato.

3. Le comunicazioni dei dati relative ai conflitti di interesse devono essere mantenute aggiornate annualmente, in occasione dell'invio delle informazioni sulla propria situazione patrimoniale e le dichiarazioni annuali dei redditi soggetti all'imposta sui redditi delle persone fisiche previste dalla legge.

4. Il dirigente deve osservare e vigilare sul rispetto delle regole in materia di incompatibilità, cumulo di impieghi e incarichi di lavoro da parte dei propri dipendenti.

5. Il dirigente svolge con diligenza le funzioni ad esso spettanti in base all'atto di conferimento dell'incarico, persegue gli obiettivi assegnati e adotta un comportamento organizzativo adeguato per l'assolvimento dell'incarico.

6. Il dirigente cura, compatibilmente con le risorse disponibili, il benessere organizzativo nella struttura alla quale è preposto, favorendo l'instaurarsi di rapporti cordiali e rispettosi tra i dipendenti, attraverso la stretta collaborazione con le Posizioni organizzative e di Alta Professionalità. Programma la formazione e all'aggiornamento del personale, l'inclusione e la valorizzazione delle differenze di genere, di età e di condizioni personali.

7. Il dirigente svolge la valutazione del personale assegnato alla struttura cui è preposto con imparzialità e rispettando le indicazioni previste nel Piano della Performance dell'Ente.

ART. 13 – RESPONSABILITA' PER VIOLAZIONE DOVERI DEL CODICE

La violazione degli obblighi previsti dal presente Codice integra comportamenti contrari ai doveri d'ufficio. Ferme restando le ipotesi in cui la violazione delle disposizioni contenute nel presente Codice, nonché dei doveri e degli obblighi previsti dal piano di prevenzione della corruzione, dà luogo anche a responsabilità penale, civile, amministrativa o contabile del pubblico dipendente, essa è fonte di responsabilità disciplinare accertata all'esito del procedimento disciplinare, nel rispetto dei principi di gradualità e proporzionalità delle sanzioni.

ART. 14 – DISPOSIZIONI FINALI

L'Amministrazione darà diffusione al presente Codice tramite la rete intranet e la pubblicazione sul proprio sito istituzionale.

Camera di Commercio
Ravenna

Regolamento interno per l'utilizzo delle tecnologie dell'informazione e della comunicazione (ICT)

In attuazione del Provvedimento dell'Autorità Garante per la protezione dei dati personali "Lavoro: le linee guida del Garante per posta elettronica e internet"
(Gazzetta Ufficiale n. 58 del 10 marzo 2007)

Art. 1 Oggetto e ambito di applicazione

1. Il presente regolamento è diretto a definire le modalità per un corretto utilizzo delle risorse informatiche della Camera di commercio di Ravenna (di seguito anche Amministrazione) anche in esecuzione di quanto previsto dagli artt. 33,34,36 del D.Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali – Capo II. Misure minime di sicurezza) e della deliberazione n. 13/2007 del Garante per la protezione dei dati personali ("Lavoro: le linee guida del Garante per posta elettronica e internet").

2. Il presente Regolamento si applica a tutti i dipendenti della Camera di commercio di Ravenna nonché a tutti coloro che, a qualsiasi titolo e quindi a prescindere dal rapporto contrattuale intrattenuto con l'Amministrazione, risultino comunque autorizzati e abilitati all'uso, anche solo occasionale e/o temporaneo, delle risorse informatiche dell'Amministrazione.

Art. 2 Definizioni

1. Ai fini del presente regolamento si intende per:

— risorse informatiche (o sistema informatico):

a) qualsiasi tipo di apparato fisico e ogni sua componente impiegato nel trattamento dei dati in forma elettronica (elaboratore, dispositivo di input o output, supporto di memorizzazione, apparato di rete e simili);

b) qualsiasi tipo di software (sistema operativo, driver, programma applicativo e simili) installato sugli apparati fisici;

c) qualsiasi tipo di servizio reso disponibile attraverso la connessione ad un sistema informatico esterno all'Amministrazione sulla base di contratti e accordi con altri enti od organizzazioni;

d) qualsiasi banca dati o informazione in formato elettronico (patrimonio informativo);

e) qualsiasi mezzo trasmissivo impiegato nella la rete locale o geografica acquisito, di proprietà, concesso in licenza d'uso o comunque nella disponibilità a qualunque titolo dell'Amministrazione;

— utente: ogni soggetto di cui all'art. 1 co.2 autorizzato all'uso delle risorse informatiche dell'Amministrazione e a tal fine fornito di specifiche credenziali di autenticazione.

— amministratore di sistema: soggetto incaricato della gestione e della manutenzione del sistema informatico, individuato dall'Amministrazione ai sensi del provvedimento del 27 novembre 2008 dell'autorità Garante per la protezione dei dati personali, previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

— rete interna: insieme degli elaboratori, degli apparati trasmissivi e degli altri apparati elettronici interconnessi tra loro e ubicati all'interno degli edifici della Camera di commercio di Ravenna comprese le sedi decentrate e le postazioni remote.

— Rete Infocamere (o IC Rete): rete geografica di trasmissione dati di proprietà di Infocamere scpa realizzata per collegare tutte le sedi principali delle Camere di Commercio e le aziende del gruppo Infocamere

Art. 3 Principi generali

1. Le risorse informatiche che l'Amministrazione mette a disposizione dei suoi utenti devono essere utilizzate nel pieno rispetto della normativa vigente e di quanto previsto dal presente

regolamento al fine di evitare possibili danni erariali, finanziari e di immagine all'Amministrazione stessa.

2. L'utilizzo delle risorse da parte degli utenti, oltre a non dover compromettere la sicurezza del sistema informatico e la riservatezza e del patrimonio informativo, non deve pregiudicare ed ostacolare le attività dell'Amministrazione od essere destinato al perseguimento di interessi previsti in contrasto con quelli pubblici.

3. Resta in ogni caso inteso che:

   a) per le risorse informatiche messe a disposizione o date in uso all'Amministrazione da altri enti od organizzazioni valgono gli accordi e le condizioni contrattuali stipulati fra le parti;

   b) per l'utilizzo di dati, software e qualunque altro tipo di contenuto riconducibile ad opera dell'ingegno valgono le norme di tutela del dritto di autore (*copyright*);

   c) l'utilizzo delle risorse informatiche dell'Amministrazione deve essere sempre e in ogni caso conforme a quanto previsto dalla normativa vigente.

4. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, a cui ha accesso e dei dati trattati a fini istituzionali. E' altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa posta a tutela dei dati personali.

5. Il datore di lavoro, a norma degli artt. 2086, 2087 e 2104 c.c. può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa e il corretto utilizzo degli strumenti di lavoro, rispettando, nell'esercizio di tali prerogative, la libertà e la dignità del lavoratore (art.4 L. n. 300/1970).

Art. 4 Attività tecnica e di manutenzione

6. L'Amministratore di sistema, il personale dell'Ufficio risorse informatiche sotto la supervisione del responsabile, il personale tecnico di società esterne contrattualmente incaricato dall'Amministrazione sotto la supervisione dell'Amministratore di sistema o del responsabile dell'Ufficio provveditorato, nonché altro personale dipendente individuato con provvedimento dirigenziale sono autorizzati ad effettuare interventi tecnici di installazione, assistenza, monitoraggio e manutenzione su ogni componente del sistema informatico dell'Amministrazione nei limiti delle proprie mansioni e competenze.

7. Il personale di cui al comma 1 può, in qualsiasi momento, previa informazione all'utente interessato, accedere, anche da remoto, alle singole postazioni di lavoro per interventi di installazione, assistenza, monitoraggio e manutenzione. Nell'effettuare tali interventi può

procedere, se necessario, alla rimozione di software e file ritenuti pericolosi per la sicurezza del sistema informatico dell'Amministrazione.

8. Nell'esercizio delle attività di cui al presente articolo, al personale di cui al comma 1 è fatto divieto di effettuare controlli indiscriminati e non giustificati da ragioni connesse al corretto ed efficiente funzionamento del sistema informatico, sull'uso, da parte dei lavoratori, degli strumenti elettronici loro assegnati.

Art. 5 Gestione delle credenziali di autenticazione

1. Le credenziali di autenticazione sono costituite da un codice identificativo personale (*username* o *user id*) e da una parola chiave (*password*). Si distinguono credenziali di accesso al *personal computer*, alla rete interna, ai servizi erogati attraverso la rete geografica IC rete e a singole applicazioni.

2. Per l'accesso al *personal computer* e alla rete interna le credenziali di autenticazione vengono attribuite direttamente dall'Ufficio risorse informatiche previa richiesta scritta (anche via posta elettronica) da parte del responsabile del servizio o dell'ufficio al quale è assegnato l'utente. Sarà cura dell'utente modificare la password al primo accesso.

3. Per l'accesso ai servizi resi disponibili attraverso la rete geografica IC rete, le credenziali vengono attribuite da Infocamere scpa. La richiesta ad Infocamere avviene per tramite dall'Ufficio risorse informatiche da parte del responsabile del servizio o dell'ufficio al quale è assegnato l'utente.

4. Le abilitazioni associate alla credenziali dell'utente sono richieste per tramite dell'Ufficio risorse informatiche da parte del responsabile del servizio o dell'ufficio al quale è assegnato l'utente.

5. Per le applicazioni e i servizi che lo consentono, le credenziali di accesso possono essere sostituite dall'utilizzo della Carta nazionale dei servizi (CNS) in combinazione con il relativo PIN. La Carta nazionale dei servizi, qualora fornita all'utente dall'Amministrazione, è nominativa, il suo uso è strettamente personale e non può essere per alcuna ragione ceduta o data in uso a terzi.

6. Per nessun apparato è consentita l'attivazione di una password all'accensione (ad esempio la password nel *bios* di un *personal computer*), senza preventiva autorizzazione da parte del Dirigente responsabile o dell'Amministratore di sistema.

7. In assenza di criteri specificamente forniti dai singoli sistemi, la password deve essere costituita da un minimo di otto caratteri di cui almeno una lettera maiuscola e almeno un carattere numerico, evitando contenuti facilmente individuabili.

8. La password deve essere personale e segreta e l'Amministratore di sistema, laddove possibile, potrà impostare opportune regole tecniche affinché la medesima sia soggetta a scadenza e debba pertanto essere cambiata periodicamente. In ogni caso l'utente dovrà cambiare la propria password al più ogni 6 mesi.

9. Deve assolutamente essere evitata la consuetudine di appuntare le proprie credenziali, per memoria, in foglietti lasciati in prossimità della propria postazione di lavoro o in documenti elettronici memorizzati in aree condivise o su supporti non protetti. Non è ammesso comunicare le proprie credenziali in risposta a richieste in qualunque modo ricevute (*email*, telefono, ecc…).

10. In caso di assenza programmata, il dipendente, in accordo con il proprio responsabile, deve preventivamente provvedere ad organizzare il lavoro d'ufficio preferibilmente con modalità che non consistano nel comunicare ai colleghi le proprie credenziali (inoltro automatico dei messaggi di posta elettronica, condivisione di file di lavoro, richiesta di abilitazioni temporanee ecc..). In alternativa l'utente può delegare un altro dipendente dell'Amministrazione (c.d. fiduciario) all'accesso a specifiche risorse con le proprie credenziali. Dell'avvenuto conferimento della delega l'utente delegante deve informare il responsabile della struttura organizzativa di appartenenza.

11. Al verificarsi di condizioni che rendano indispensabile e indifferibile utilizzare specifiche credenziali il cui titolare è temporaneamente o definitivamente indisponibile, il Dirigente responsabile potrà dare disposizioni all'Amministratore di sistema di mettere in atto quanto necessario al superamento della procedura di autenticazione (forzatura della password). Dell'operazione dovrà essere data comunicazione al titolare interessato appena possibile.

12. Alla cessazione del rapporto intrattenuto con l'Amministrazione, o al venire meno della necessità di utilizzo di specifiche risorse, l'utente o il responsabile della struttura organizzativa di appartenenza, deve inoltrare all'Ufficio risorse informatiche richiesta scritta di disattivazione delle credenziali o di disabilitazione delle stesse ai servizi non più necessari.

Art. 6 Utilizzo del personal computer

1. Il personal computer e l'insieme degli altri dispositivi che completano la postazione di lavoro sono affidati all'utente per ragioni di ufficio. Essi costituiscono strumento di lavoro e, in quanto tale, devono essere utilizzati con cura ed esclusivamente per finalità relative allo svolgimento dell'attività lavorativa.

2. Sui personal computer, così come su qualsiasi altro dispositivo che lo consenta (*server*, computer portatile, *tablet*, *smartphone* e simili), è vietata l'installazione di qualunque tipo di *software* (*firmware*, *software* di base, *driver* e programmi operativi) diverso da quello regolarmente presente in quanto pre-installato o installato dal personale di cui all'art. 4 co 1. a ciò autorizzato. L'inosservanza della presente disposizione espone l'Amministrazione a gravi

rischi in relazione alla sicurezza del sistema informatico e alla riservatezza del patrimonio informativo. Inoltre l'installazione di software non regolarmente licenziato può integrare fattispecie di reato o di illecito amministrativo.

3. L'Amministrazione si riserva di attribuire agli utenti credenziali di accesso non abilitate alla installazione di software e alla modifica della configurazione del *personal computer* e degli altri dispositivi che completano la postazione di lavoro.

4. Ogni utente deve adottare comportamenti adeguati a preservare il buon funzionamento del *personal computer* e degli altri dispositivi in dotazione. A tal fine, e con l'obiettivo di ridurre i rischi per la sicurezza del sistema informatico, l'utente deve attenersi alle seguenti disposizioni:

   a) non cedere, una volta superata la fase di autenticazione, l'uso della propria postazione di lavoro a personale non autorizzato;

   b) non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;

   c) bloccare il *personal computer* in caso di allontanamento temporaneo dalla propria postazione di lavoro, al fine di evitare l'indebito utilizzo da parte di terzi (per il sistema operativo *windows* utilizzare il comando CTRL-ALT- CANC e "blocca computer")

   d) spegnere il *personal computer* e ogni altro dispositivo elettronico al termine dell'attività lavorativa;

   e) non installare, senza autorizzazione, dispositivi che sfruttino il sistema di comunicazione telefonico per l'accesso a internet o a banche dati esterne (quali *modem* e *internet key*);

   f) limitare l'uso di supporti di memorizzazione rimovibili (cd/dvd, chiavette USB, *memory card*, *hard disk* esterni e simili) alle strette esigenze di servizio e a dispositivi di provenienza sicura, preventivamente controllati con software antivirus;

   g) astenersi dal modificare le configurazioni (*hardware* e *software*) dei dispositivi forniti come impostate all'atto dell'assegnazione o a seguito di successivi interventi da parte del personale di cui all'art 4 co. 1;

   h) segnalare tempestivamente all'Ufficio risorse informatiche l'eventuale danneggiamento o malfunzionamento dei dispositivi assegnati anche in via temporanea.

5. L'utilizzo di un dispositivo mobile (*computer* portatile, *tablet*, *smartphone* e simili) eventualmente assegnato all'Utente, anche per un periodo di tempo limitato, segue le stesse regole previste per i *personal computer*. L'utente assegnatario deve custodire il dispositivo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Qualora si tratti di

un'assegnazione temporanea l'utente assegnatario deve provvedere alla rimozione di eventuali file memorizzati sul dispositivo mobile prima della riconsegna all'ufficio che lo ha in dotazione.

6. Ciascun responsabile di ufficio/servizio è tenuto a verificare il corretto utilizzo delle risorse assegnate in dotazione alla propria struttura.

Art. 7 Utilizzo e conservazione dei supporti di memorizzazione rimovibili

1. Tutti i supporti di memorizzazione rimovibili (CD/DVD, chiavette USB, *memory card*, *hard disk* esterni e simili), contenenti dati personali, soprattutto se sensibili, nonché dati costituenti patrimonio informativo riservato dell' amministrazione, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, alterato, distrutto o, successivamente alla cancellazione, recuperato.

2. Al fine di assicurare la definitiva rimozione del contenuto e/o la distruzione dei supporti di cui al precedente comma, l'utente dovrà contattare l'Ufficio risorse informatiche e seguire le istruzioni da questo impartite.

3. In ogni caso, i supporti contenenti dati personali devono essere adeguatamente custoditi in armadi chiusi o, comunque, in luoghi non facilmente accessibili a terzi.

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

Art. 8 Utilizzo delle stampanti e dei materiali di consumo

1. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, *toner*, supporti magnetici, supporti digitali) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

2. Per ragioni di efficienza ed economicità, dove possibile, devono essere privilegiati:

   a) la diffusione e la comunicazione di documenti in formato elettronico, selezionando il mezzo più opportuno in relazione alla natura del documento (posta elettronica, posta elettronica certificata, portale istituzionale, portale intranet, rete interna, sistemi di *file hosting* o altro strumento autorizzato), rispetto alla diffusione e alla comunicazione di documenti in formato cartaceo;

   b) l'uso delle stampanti di rete rispetto all'uso della stampante, se presente, installata in locale;

   c) la modalità di stampa fronte/retro rispetto alla modalità solo fronte;

   d) la stampa in bianco e nero rispetto alla stampa a colori.

3. I materiali di consumo devono essere trattati e smaltiti sulla base delle istruzioni impartite dall'Amministrazione.

Art. 9 Utilizzo della rete interna

1. E' assolutamente vietato accedere a qualunque risorsa resa disponibile dall'Amministrazione attraverso la rete interna con credenziali diverse da quelle assegnate. L'accesso alle risorse di rete è soggetto ad attività di tracciamento elettronico automatico (con informazioni memorizzate nei cosiddetti *file* di *log*).

2. Le cartelle accedibili attraverso rete interna (servizio di *file server*), di norma visualizzate come unità di rete, costituiscono aree di condivisione e conservazione sicura di *file* attinenti l'attività lavorativa. Pertanto non può esservi collocato nessun *file* di carattere personale o comunque estraneo all'attività d'ufficio nemmeno per brevi periodi. Le cartelle di rete sono soggette a regolari attività di controllo, amministrazione e *back-up* da parte del personale dell'Ufficio risorse informatiche anche con procedure automatiche.

3. I dischi interni ai personal computer o eventuali altre unità di memorizzazione rimovibili non sono sottoposti a procedure di *back-up* centralizzate. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente. L'Amministrazione provvede a mettere a disposizione dell'Utente, previa richiesta, opportune aree del *file server* dedicate al salvataggio dei dati o, in alternativa, supporti magnetici o dischi ottici (CD/DVD) qualora il *personal computer* sia dotato di unità di masterizzazione.

4. Il personale dell'Ufficio risorse informatiche può, in qualunque momento, procedere alla rimozione dalle cartelle di rete di ogni contenuto che ritiene non pertinente l'attività d'ufficio e/o pericoloso per la sicurezza del sistema informatico. Al di fuori dei casi di urgenza il suddetto personale interviene solo previa comunicazione agli utenti interessati.

5. Nell'uso delle cartelle di rete da parte degli utenti, particolare attenzione deve essere prestata nel selezionare i dati da collocarvi in base a reali esigenze di condivisione e conservazione, essendo infatti necessario evitare un'archiviazione eccessiva e ridondante. Risulta inoltre opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda al controllo dei dati di propria pertinenza memorizzati nelle cartelle di rete, rimuovendo i *file* obsoleti, duplicati o la cui collocazione in rete è divenuta, per qualsiasi ragione, superflua.

6. Per tutte le altre risorse rese disponibili attraverso la rete interna (quali ad esempio il portale Intranet o il servizio fax) valgono le istruzioni e le condizioni di utilizzo impartite dall'Amministrazione al di fuori del presente Regolamento.

Art. 10 Utilizzo di Internet

1. L'utilizzo di Internet è consentito esclusivamente per finalità di servizio e mediante le attrezzature informatiche messe a disposizione dall'Amministrazione. E' assolutamente vietato l'accesso con credenziali di autenticazione differenti da quelle assegnate.

2. In deroga al comma 1, è autorizzato l'uso di Internet per l'assolvimento di incombenze amministrative o burocratiche, per il tempo strettamente necessario allo svolgimento delle relative operazioni, quali ad esempio adempimenti *on-line* nei confronti di pubbliche amministrazioni o concessionari di pubblici servizi; rapporti con istituti bancari o assicurativi.

3. La connettività ad Internet è fornita da Infocamere scpa attraverso IC rete. Fatta esclusione per i dispositivi mobili (portatili, *smartphone*, *tablet* e simili), quando non connessi alla rete interna, non è consentito utilizzare *Internet service provider* (ISP) diversi da Infocamere con sistemi di connessione diversi da IC rete a meno di esplicita autorizzazione.

4. A titolo esemplificativo e non esaustivo, si ritengono non ammissibili le seguenti attività:

a) la navigazione, la registrazione e ogni altra operazione in siti che non abbiano attinenza con l'attività lavorativa fatta eccezione per quanto previsto al comma 2;

b) il *download* (scaricamento) o l'*upload* (caricamento) di file non necessari allo svolgimento delle prestazioni professionali così come, più in generale, tutte le attività che possano causare malfunzionamento, diminuiscano la regolare operatività, distraggano risorse, danneggino o restringano l'utilizzabilità o le prestazioni della rete interna o di IC rete;

c) le attività poste in essere con l'intento di violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni, intercettare, tentare d'intercettare o accedere a dati, in transito sulla rete, dei quali non si è destinatari;

d) la commissione di qualunque atto, compiuto attraverso la rete, che integri fattispecie di reato (per esempio in materia di tutela del diritto d'autore), possa recare danno a terzi o ledere l'immagine dell'Amministrazione;

e) la partecipazione *social network*, *forum* non professionali, bacheche elettroniche, sistemi di messaggeria istantanea (*chat*) se non espressamente autorizzati;

f) l'utilizzazione di sistemi *peer to peer* (quali ad esempio BitTorrent o eMule), di *file sharing* (condivisione di file) o similari,

g) la connessione a siti che trasmettono in *streaming* (come radio o TV via WEB), fatti salvi i casi riconducibili a specifiche e motivate ragioni di servizio.

5. L'Amministrazione, nell'ambito della propria attività istituzionale, potrà sperimentare e realizzare forme evolute di comunicazione in rete (quali *forum* e *social network*) basate sulla creazione e lo scambio di informazioni all'interno di una comunità virtuale. In tal caso, gli utenti

che partecipano alla comunità virtuale sono responsabili del contenuto dei propri messaggi e rispondono personalmente delle violazioni delle norme di comportamento che andranno ad integrare il presente Regolamento.

6. Al fine di evitare un utilizzo di Internet non pertinente all'attività lavorativa, l'Amministrazione può adottare uno specifico sistema di *web filtering* (blocco selettivo di contenuti) che consente di impostare limiti alla navigazione (*policy*) in base ai tipi di contenuto, ai tipi di *file* visualizzati e/o scaricati, ai protocolli di rete, agli utenti o gruppi di utenti .

7. L'Amministrazione si riserva la possibilità di accedere ai dati relativi alle operazioni di accesso e navigazione Internet poste in essere dagli utenti. Tali dati vengono automaticamente memorizzati in formato elettronico dal fornitore di connettività nei cosiddetti file di *log* e conservati nei modi e per il periodo di tempo previsti dalla legge.

8. Il trattamento dei dati contenuti nei file di *log* da parte dell'Amministrazione avviene di norma in forma aggregata o anonima in modo tale da precludere l'immediata identificazione degli utenti e/o delle loro attività. I dati personali contenuti nei *file* di *log* possono essere trattati in via eccezionale solo ove ricorrano una o più delle seguenti ipotesi:

   a) per corrispondere ad eventuali specifiche richieste di informazioni da parte dell'Autorità giudiziaria;

   b) quando si verifichi un evento dannoso o una situazione di pericolo che richiedano un immediato e necessario intervento;

   c) qualora l'utilizzo anomalo degli strumenti elettronici, nonostante le contromisure adottate dall'Amministrazione in via anonima o aggregata per l'eliminazione delle relative cause (in particolare, utilizzo di sistemi di *web filtering* o avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia), risulti tuttavia persistente, costituendo perciò stesso un pericolo per la sicurezza del sistema e/o per il regolare funzionamento delle attività di ufficio e/o, ancora, qualora lo stesso utilizzo anomalo degli strumenti elettronici possa integrare fattispecie di responsabilità sotto il profilo disciplinare; amministrativo-contabile; civile e/o penale.

9. L'eventuale prolungamento dei tempi di conservazione dei dati di cui al comma 7 da parte dell'Amministrazione riveste carattere eccezionale ed è consentito esclusivamente per il tempo strettamente necessario nella ipotesi di cui al comma 8 e limitatamente alle sole informazioni ritenute indispensabili.

Art. 11 Utilizzo della posta elettronica

1. La casella di posta elettronica assegnate individualmente al singolo Utente (di norma *nome.cognome*@ra.camcom.it), così come le caselle istituzionali (di norma *struttura*@ra.camcom.it) cui l'utente ha accesso, costituiscono strumento di lavoro e, pertanto, sono esclusivamente utilizzabili per finalità. di servizio.

2. Per l'utilizzo e il valore giuridico della posta elettronica (ordinaria e certificata) nelle attività istituzionali, nonché per le regole di protocollazione informatica dei messaggi trasmessi e ricevuti attraverso la posta elettronica vale quanto previsto nel Manuale di gestione documentaria adottato dall'Amministrazione a cui si rimanda.

3. Trattandosi di strumento ad uso esclusivo di lavoro, a titolo esemplificativo e non esaustivo, è vietato l'uso della casella di posta assegnata nominativamente all'utente, così come di altra casella di posta istituzionale cui l'utente accede, per:

   a) la propagazione a catena di messaggi (le cosiddette "catene di Sant'Antonio"), l'invio o l'inoltro di messaggi pubblicitari, di offerte commerciali, di proposte di vendita e simili (il cosiddetto "*spam*");

   b) la partecipazione a dibattiti di natura non professionale, ad appelli e/o petizioni (anche se possono sembrare veritieri e/o socialmente utili), a giochi o a qualsivoglia altra attività non riconducibile allo svolgimento dell'attività lavorativa;

   c) l'apertura di *link* contenuti nel testo del messaggio o di file trasmessi in allegato, in presenza di elementi (quali, ad esempio, mittente sconosciuto o assente, contenuto del messaggio incongruo o privo di significato, richieste di dati immotivate, riferimenti a inesistenti transazioni finanziarie o commerciali, file allegato di tipo eseguibile o con estensione non conosciuta ecc..). che facciano ritenere tali operazioni pericolose per la sicurezza del sistema informatico o destinate a carpire informazioni riservate. In caso di *link* o file sospetti è opportuno avvalersi del supporto dell'Ufficio risorse informatiche;

   d) l'invio in allegato al testo delle proprie comunicazioni di file potenzialmente dannosi per il sistema informatico dell'Amministrazione o del ricevente (quali file eseguibili o contenenti macro), così come file di dimensioni eccessive;

   e) l'invio di documenti e informazioni riservati nonché di dati personali senza l'autorizzazione da parte responsabile o titolare del trattamento, ad esclusione di quanto previsto da specifici regolamenti o consentito dalla normativa in materia di protezione dei dati personali;

   f) la trasmissione di informazioni con contenuti contrari a norme di legge, non veritieri, offensivi, discriminatori e/o diffamatori o che possano costituire comunque fonte di responsabilità per l'Amministrazione;

g) in ogni altro caso in cui l'utilizzo della casella di posta assegnata risulti palesemente incoerente con la prestazione lavorativa o in contrasto con la sicurezza del sistema informatico.

4. In caso di assenza prolungata, l'utente può provvedere, in accordo con il responsabile dell'ufficio o del servizio, ad impostare un inoltro automatico dei messaggi ad altra casella di posta elettronica interna o messaggi automatici di risposta contenenti riferimenti alternativi (indirizzi elettronici o telefonici) o altre utili modalità di contatto della struttura. Tali soluzioni sono da preferire a quella, comunque consentita, consistente nel delegare un altro utente (c.d. fiduciario) a verificare il contenuto dei messaggi di posta elettronica e a inoltrare al responsabile dell'ufficio di appartenenza quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

5. In caso di assenza prolungata e non programmata (ad es. per malattia) una qualunque delle procedure di cui al precedente comma 4, qualora non possa essere attivata dal lavoratore avvalendosi del servizio *webmail,* potrà essere attivata a cura dell'Amministrazione, su espressa richiesta dell'interessato o del Dirigente responsabile, previa (se possibile) comunicazione all'utente interessato medesimo, per garantire il regolare andamento delle attività dell'Ufficio.

6. L'inoltro dei messaggi ad un'altra casella di posta avviene, altresì, in occasione di cessazione del rapporto intrattenuto dall'utente con l'Amministrazione. Si procederà, in tal caso, anche all'eliminazione della casella dell'Utente cessato, a seguito di richiesta del responsabile del Servizio di riferimento.

Art. 12 Controlli

1. Nel rispetto dei principi di "non eccedenza" e di "pertinenza" (art. 11 del decreto legislativo 30 giugno 2003. n. 196) i controlli sull'uso di strumenti elettronici che possano determinare il trattamento di dati personali riferibili al singolo utente, saranno prioritariamente di tipo aggregato, riferiti all'intera struttura lavorativa dell'amministrazione o a sue aree, quindi di tipo anonimo, e si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevala l'anomalia, nei quali sì evidenzierà l'utilizzo irregolare degli strumenti elettronici e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

2. L'Amministrazione procederà a controlli su base individuale qualora le anomalie, nonostante le contromisure adottate per l'eliminazione delle relative cause, risultino tuttavia persistenti, costituendo un pericolo per la sicurezza del sistema c/o per il regolare funzionamento delle attività di ufficio e/o, ancora, qualora l'utilizzo anomalo degli strumenti elettronici rilevato in sede di controllo possa integrare eventuali fattispecie di responsabilità sotto il profilo disciplinare, amministrativo-contabile, civile.

Art. 13 Sanzioni

1. Il presente Regolamento riveste valenza e natura di codice comportamentale e, quindi, è fatto obbligo a tutti gli utenti di un suo puntuale rispetto. La violazione delle disposizioni di cui al presente Regolamento è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari, nelle forme e secondo le procedure previste dal vigente CCNL. nonché sotto il profilo civile, penale e/o amministrativo-contabile, laddove ne ricorrano i presupposti di legge.

2. La contravvenzione alle regole contenute nel presente Regolamento può comportare la revisione e la revoca, temporanea o permanente, delle autorizzazioni ad accedere alle risorse informatiche gestite dall'Amministrazione, fatte salve le più gravi conseguenze di cui al comma 1.

3. Con riferimento ai collaboratori e al personale comunque estraneo all'Amministrazione, qualora questi, per l'espletamento dei rispettivi incarichi, siano autorizzati a utilizzare gli strumenti elettronici considerati dal presente Regolamento, nell'ambito dei contratti e provvedimenti di conferimento dei relativi incarichi dovrà essere inserita un'espressa clausola che imponga l'obbligo in capo agli stessi lavoratori di rispettare il Regolamento in questione, con previsione del diritto dell'Amministrazione, nei casi di violazione accertata di particolare gravità, di risolvere il contratto stesso, con salvezza di ogni eventuale azione civile e/o penale a carico del contraente inadempiente, laddove ne ricorrano i presupposti di legge.

IL SEGRETARIO GENERALE
Dott.ssa Paola Morigi
Documento Firmato Digitalmente