CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA - TRENTO

DISCIPLINARE

PER L'UTILIZZO

DELLE ATTREZZATURE INFORMATICHE

E TELEFONICHE

DELLA POSTA ELETTRONICA E

DELLA RETE INTERNET

Adottato con deliberazione della Giunta camerale n. 70 di data 6/8/2012

SOMMARIO

CAPO I
OGGETTO, FINALITA' E DESTINATARI

1. Oggetto e finalità

1.1 Il presente Disciplinare, adottato con provvedimento della Giunta della Camera di Commercio I.A.A. di Trento nel rispetto di quanto previsto dal D.Lgs. 7 marzo 2005 n. 82 (Codice dell'amministrazione digitale), dal D.Lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali), della legge 20 maggio 1970, n. 300 (Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento), dell'art. 24 della Legge 29 marzo 1983, n. 93 "Legge quadro sul pubblico impiego", nonché secondo le indicazioni contenute nella deliberazione 1 marzo 2007 n. 13 del Garante per la protezione dei dati personali, recante "Linee guida del Garante per posta elettronica e internet", ha per oggetto i criteri e le modalità operative di accesso e utilizzo del servizio internet, di posta elettronica, delle attrezzature informatiche e telefoniche appartenenti all'Ente camerale.

1.2 L'adozione di queste misure ha lo scopo di garantire la disponibilità e l'integrità dei sistemi informativi e di comunicazione della Camera di Commercio nonché la sicurezza sul lavoro. Il rispetto del Disciplinare assicura, in particolare:
a) la riservatezza delle informazioni e dei dati trattati dall'Ente camerale;
b) la massima sicurezza nello scambio di tali dati e informazioni;
c) la massima efficienza delle risorse informatiche e del loro utilizzo;
d) la continuità dei servizi informatici camerali;
e) il rispetto delle leggi in materia di utilizzo delle risorse informatiche e telefoniche.

1.3 A tal fine, l'Ente camerale adotta, nel rispetto delle libertà fondamentali e della dignità dei lavoratori, idonee misure di sicurezza e organizzative, fermo restando il divieto di utilizzo sistematico di sistemi *hardware* e *software* preordinati al solo fine del controllo a distanza dell'attività lavorativa del dipendente.

2. Destinatari

2.1 Il presente Disciplinare si applica:
a) ai dipendenti della Camera di Commercio I.A.A. di Trento dell'area dirigenziale e non dirigenziale;
b) agli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture dell'Ente camerale (ad esempio: collaboratori e tirocinanti), in quanto compatibile.

2.2 I contenuti del presente disciplinare costituiscono, inoltre, linee guida per il corretto utilizzo tecnico delle strumentazioni informatiche per coloro che, a qualunque titolo, utilizzano il *sistema informativo* camerale.

2.3 Per praticità, nel Disciplinare si indica indistintamente con i termini "dipendente", "*assegnatario*", "consegnatario" o "*utente*" i soggetti autorizzati a qualsiasi titolo dall'Ente camerale ad utilizzare le risorse e le attrezzature informatiche e telefoniche.

3. Responsabilità

3.1 Tutti i soggetti di cui al precedente punto 2 sono responsabili per ciò che concerne:
a) il rispetto del presente Disciplinare;
b) l'uso esclusivo delle proprie *credenziali di autenticazione*;
c) l'adozione degli accorgimenti operativi utili ad accrescere la protezione della propria connessione a internet e alla casella di posta elettronica in modo da ridurne i rischi in termini di sicurezza e privacy;

d) la segnalazione senza ritardo al superiore gerarchico di ogni eventuale attività non autorizzata di cui siano venuti a conoscenza per motivi d'ufficio.

3.2 Ogni infrazione alle regole emanate dall'Ente camerale per un uso corretto del *sistema informatico* e telefonico costituirà una violazione della sicurezza ed esporrà il dipendente all'applicazione dei provvedimenti disciplinari previsti dal contratto collettivo di lavoro, fermo restando l'obbligo di segnalazione alla competente Autorità giudiziaria per l'accertamento della responsabilità personale, civile e penale, nei casi previsti dalla legge.

3.3 Tutti i soggetti di cui al precedente punto 2 devono ottenere l'autorizzazione dell'Ente camerale prima di intraprendere qualsiasi attività non esplicitamente disciplinata dalle disposizioni che seguono, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Ente camerale.

4. Titolarità

4.1 La Camera di Commercio I.A.A. di Trento è proprietaria di tutti i dati e le informazioni archiviate negli elaboratori e nei sistemi di comunicazione dell'Ente camerale, inclusi i messaggi di posta elettronica e i *file* salvati nelle cartelle di lavoro assegnate in via esclusiva a ciascun utente.

CAPO II
ATTREZZATURE INFORMATICHE, POSTA ELETTRONICA E INTERNET

Titolo I
Attrezzature e servizi di natura informatica

5. Finalità di utilizzo delle attrezzature informatiche

5.1 Ai fini del presente disciplinare, per attrezzature informatiche si intendono tutti i dispositivi ad uso informatico, quali personal computer, portatili-laptop, thin *client*, periferiche di memorizzazione dati (*penne usb*, lettori cd-dvd, dischi esterni, ecc...), palmari, smartphone, periferiche di stampa ed acquisizione (stampanti e scanner multifunzione, ecc.) ed altre apparecchiature che si possono interfacciare con la rete camerale.

5.2 Le attrezzature informatiche assegnate dall'Ente camerale ai dipendenti sono conformi alla normativa vigente in materia di sicurezza delle apparecchiature. Esse rimangono di proprietà della Camera di Commercio I.A.A. di Trento.

5.3 Salvo quanto previsto al Titolo IV del presente Capo II, ogni utilizzo delle attrezzature informatiche per finalità estranee all'attività di servizio è vietato.

5.4 La violazione degli obblighi di cui al presente Titolo comporterà l'intervento dell'Ente camerale finalizzato al ripristino della corretta gestione dei beni, fermo restando l'obbligo di segnalare alla competente Autorità giudiziaria l'accertamento della responsabilità personale, civile e penale, dell'*assegnatario* delle attrezzature, nei casi previsti dalla legge.

6. Modalità di utilizzo delle attrezzature informatiche

6.1 L'accesso al *sistema informatico* dell'Amministrazione è vincolato all'attivazione delle credenziali informatiche da parte dell'Ufficio Sistemi Informatici dietro presentazione dell'apposita scheda tecnica di cui all'Allegato n. 1 ed è subordinato all'utilizzo di un codice di identificazione e di una password.

6.2 La password è strettamente personale e di uso esclusivo dell'*utente* e ha una durata massima di 90 giorni. Quindici giorni prima della scadenza, l'*utente* è avvisato della necessità di sostituire la password. La password deve rispettare le regole riportate nella sezione 'cambio password' della Intranet camerale.
Nel caso in cui la password abbia perso il requisito dell'assoluta riservatezza il dipendente è tenuto a sostituirla immediatamente ed a comunicarlo ove necessario all'*Amministratore di sistema* [cfr. Appendice B – Glossario, voce: *Amministratore di Sistema*].
L'accesso ai dati effettuato da persona non autorizzata che utilizza la password altrui costituisce illecito (accesso abusivo a *sistema informatico* – art. 615 ter C.P.), e comporta l'attribuzione della responsabilità del trattamento effettuato abusivamente anche a colui il quale ha volontariamente o inavvertitamente ceduto o resa conoscibile la propria password.

6.3 Nell'uso delle attrezzature informatiche assegnate, il dipendente deve rispettare le seguenti disposizioni:

a) è vietato ogni tipo di modifica (aggiunta, rimozione, sostituzione) dei componenti interni delle apparecchiature informatiche, essendo tali operazioni di competenza esclusiva dell'Ufficio Sistemi Informatici;
b) nessun *utente* non espressamente autorizzato può installare sulle apparecchiature informatiche *software* diversi da quelli compresi nella dotazione base o modificarne la configurazione, senza il preventivo consenso dell'*Amministratore di sistema*;
c) l'*utente* è responsabile delle attrezzature che gli sono affidate in uso e, pertanto, deve provvedere a mantenerle in completa efficienza segnalando tempestivamente all'Ufficio Sistemi Informatici, tramite il referente informatico, ogni eventuale problema tecnico ed eventuali dubbi sulla sicurezza della postazione informatica;
d) le attrezzature informatiche possono essere utilizzate soltanto dal legittimo *assegnatario*; è quindi tassativamente escluso l'utilizzo da parte di terzi non autorizzati;
e) in caso di furto o smarrimento di attrezzature, gli assegnatari hanno l'obbligo di informare tempestivamente l'Ufficio Economato, il quale provvederà alla denuncia presso l'autorità competente. In tali evenienze, l'*assegnatario* dovrà darne comunicazione anche all'Ufficio Sistemi Informatici;
f) nelle sedi camerali non è consentito l'uso di attrezzature informatiche private ed in connessione con la rete dati camerale;
g) è vietato ai dipendenti non autorizzati l'accesso ai locali in cui sono custoditi i *server*.

6.4 Riguardo alla memorizzazione dei dati, gli utenti devono rispettare le seguenti disposizioni:

a) tutti i dati dell'Ente camerale devono risiedere sui dischi magnetici dei *server* di rete e su *storage* dedicati all'interno di cartelle e sottocartelle organizzate in maniera logica e gerarchica. In particolare:
   - la cartella denominata "Cartella comune", suddivisa in numerose sottocartelle destinate ai singoli uffici, è accessibile a tutti i dipendenti appartenenti ai diversi uffici che necessitano di accedere o scambiare dei *files*; i dati sensibili, giudiziari e quelli riservati non devono transitare nella "Cartella comune"; i *files* di mero scambio devono essere cancellati subito dopo il trasferimento;
   - di norma, i dipendenti di un ufficio (o unità organizzativa) hanno accesso solo alle cartelle dell'ufficio (o unità organizzativa) cui sono assegnati in base ai diritti di accesso loro attribuiti dal Responsabile del trattamento (Dirigente d'Area) per il tramite del Responsabile di U.O. (Direttore d'Ufficio);

- i dipendenti di un ufficio (o unità organizzativa) possono avere accesso alle cartelle di altri uffici (o unità organizzative) in base ai diritti loro concessi dai rispettivi Responsabili di trattamento;

b) ciascun dipendente ha accesso ad alcune cartelle i cui diritti di accesso sono assegnati in via esclusiva e non condivisa con alcuno, fatto salvo l'*Amministratore di sistema* che debba intervenire per scopi di manutenzione tecnica; anche questa cartella deve contenere esclusivamente documenti attinenti l'attività lavorativa;

c) tutti i dati che risiedono sui *server* della rete camerale sono soggetti a procedure automatizzate di *backup* gestite e monitorate dall'*Amministratore di sistema*;

d) è vietato l'utilizzo, salvo autorizzazione dell'*Amministratore di sistema*, di password di *file*.

6.5 I supporti di memorizzazione removibili (CD, DVD, memorie di massa, *USB*, etc.) sono dati in uso ai dipendenti che li richiedono per scopi legati all'attività lavorativa. In relazione al loro utilizzo, i dipendenti devono rispettare le seguenti prescrizioni:

a) formattare i supporti informatici removibili e riscrivibili, prima del loro riutilizzo ex novo;

b) collegare tali supporti esclusivamente ad attrezzature informatiche dotate di protezioni antivirus attive ed aggiornate unicamente all'interno del *sistema informativo* camerale al fine di impedire la diffusione di virus informatici. Tali supporti non possono essere ad esempio utilizzati per il trasferimento di *file* dall'Ufficio a casa e viceversa;

c) utilizzare i supporti removibili per il trasferimento dati e non per l'archiviazione degli stessi;

d) poiché i dati devono sempre risiedere su *server* di rete muniti di sistema di *backup*, eseguire appena possibile l'operazione di salvataggio sul *server*; dopo il trasferimento i dati memorizzati nei supporti di cui trattasi devono essere eliminati;

e) proteggere con password le *penne USB* che lo permettono;

f) custodire i supporti con diligenza in luoghi sicuri (cassaforte o armadi dotati di serratura), inaccessibili a persone non autorizzate al trattamento dei dati, in modo da evitarne lo smarrimento o il furto;

g) prima della consegna a terzi del supporto di memoria, procedere alla cancellazione delle informazioni precedentemente contenute rispetto a quelle che si desidera trasmettere;

h) nel caso in cui il supporto non fosse più utilizzabile, distruggerlo con strumenti idonei.

6.6 Per il corretto trattamento di dati con strumenti informatici, il lavoratore deve:

a) adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale di autorizzazione (divieto di rendere note ad altre persone le password e di condividerle). Il dipendente deve, in particolare, evitare di trascrivere le password su supporti facilmente accessibili a terzi;

b) non lasciare incustodito e accessibile lo strumento elettronico durante la sessione di lavoro;

c) rispettare le modalità previste per la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento;

d) rispettare i divieti, gli obblighi e le prescrizioni disposte in materia contenute nelle Linee guida per la sicurezza nel trattamento dei dati personali adottate dall'Ente camerale e consegnate a ciascun dipendente.

6.7 In caso di cessazione del rapporto di lavoro, l'*assegnatario* delle attrezzature informatiche deve presentare all'Ufficio Sistemi Informatici, per il tramite del proprio Direttore d'Ufficio, richiesta di disattivazione delle proprie *credenziali di autenticazione*

dichiarando di aver provveduto alla cancellazione definitiva dei dati personali dal *sistema informativo* camerale (cfr. Allegato n. 2). L'Ufficio Sistemi Informatici provvederà alla disattivazione nei tempi e modi previsti.

6.8 L'Ente camerale non si rende in nessun caso responsabile per danni recati a terzi causati dall'uso scorretto delle attrezzature informatiche da parte dell'*assegnatario* delle attrezzature stesse, in particolare dall'uso non conforme alle disposizioni del presente Disciplinare.

7. Modalità di manutenzione delle attrezzature e di assistenza informatica

7.1 Nel caso di interventi di manutenzione e/o di assistenza sulla postazione fisica è necessario garantire presso la postazione di lavoro la presenza dell'*utente* o del referente informatico o, in loro assenza, di altro dipendente dell'unità organizzativa individuato dal Responsabile della medesima.

7.2 L'*assegnatario* delle attrezzature informatiche è tenuto a mettere immediatamente a disposizione dell'Ente camerale tutta l'attrezzatura ricevuta in via definitiva o temporanea, per interventi di manutenzione ed in ogni caso di motivata richiesta; è tenuto altresì a restituire l'attrezzatura integra – salva l'obsolescenza dovuta all'uso – in caso di cessazione del titolo per il quale l'attrezzatura è stata assegnata.

7.3 L'*Amministratore di sistema* può utilizzare, sentite le Organizzazioni Sindacali ai sensi dell'art. 24 della Legge 29 marzo 1983, n. 93 "Legge quadro sul pubblico impiego", i *software* di assistenza remota descritti nell'Allegato n. 3, nel rispetto della normativa vigente e, in particolare, dell'art. 4 della Legge 30 maggio 1970, n. 300 "Statuto dei lavoratori", che reca l'obbligo di non adibire tali strumenti a finalità di controllo a distanza dei lavoratori e del D.Lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali."

7.4 L'*Amministratore di sistema* è appositamente istruito in merito a compiti, limiti e responsabilità di intervento relativamente all'uso della metodologia di assistenza a distanza.

7.5 L'*Amministratore di sistema,* al quale perviene una richiesta di assistenza a distanza inoltrata da un *utente*, è abilitato a provvedere solamente se il dipendente medesimo esprimerà, per mezzo di una procedura informatizzata, il proprio consenso affinché l'operatore informatico assuma il controllo della postazione allo scopo di verificare gli inconvenienti segnalati e provvedere alla loro soluzione; mentre l'*Amministratore di sistema* svolge i servizi in assistenza remota, il dipendente può osservare in tempo reale sul proprio schermo ogni azione compiuta dal tecnico.

7.6 Nel caso in cui il *software* predisposto per l'assistenza remota abbia eventuali disfunzioni tecniche nella richiesta preventiva di autorizzazione dell'accesso, l'*Amministratore di sistema* chiede l'autorizzazione almeno verbalmente e l'*utente* dispone comunque di una segnalazione visiva circa l'attivazione dell'avvenuta connessione.

7.7 Derogano alle disposizioni di cui al presente punto le postazioni non presidiate da un assegnatario, la cui manutenzione a distanza deve essere garantita per motivi di continuità di servizio.

8. Modalità di utilizzo delle postazioni informatiche mobili

8.1 L'assegnazione dell'attrezzatura per lavoro mobile è subordinata alla sottoscrizione della scheda tecnica riportata nell'Allegato n. 4.

8.2 I dipendenti assegnatari utilizzano l'attrezzatura per lavoro mobile esclusivamente per gli scopi cui sono diretti: evitano di connettersi, salvo necessità di servizio, a reti diverse da quella camerale, verificando in ogni caso, con metodologie condivise con l'Ufficio

Sistemi Informatici, l'aggiornamento della protezione antivirus almeno una volta alla settimana.

8.3 L'*assegnatario* dell'attrezzatura è tenuto ad adottare la massima diligenza nell'uso e conservazione delle attrezzature per il lavoro mobile ricevute in consegna, con particolare riguardo alla loro custodia in caso di uso esterno e in luoghi pubblici.

8.4 L'*assegnatario* dell'attrezzatura è unico responsabile per furti, danneggiamenti ed alterazioni, sia fisiche che logiche, subiti per propria colpa dalle attrezzature mobili ricevute in consegna, per i quali è obbligato a corrispondere all'Ente camerale un giusto valore di mercato pattuito a consuntivo, al fine di ristabilire la piena utilità ed integrità dei beni all'origine assegnati.

8.5 L'*assegnatario* è unico responsabile di ogni trattamento di dati personali, in ogni sua forma, compresa la memorizzazione, la protezione, il *backup*, il *disaster recovery* ed altro, che risulti necessario effettuare sulla postazione mobile assegnata. E' pertanto a cura esclusiva dell'*assegnatario* l'adozione di ogni modalità operativa utile per un consapevole utilizzo della postazione mobile ai fini della normativa vigente in tema di sicurezza informatica, trattamento di dati personali e diritto d'autore.
In particolare, sul disco fisso del portatile possono essere temporaneamente mantenuti solamente i dati necessari ed esclusivamente per il tempo strettamente indispensabile al loro utilizzo; tali dati devono essere trasferiti appena possibile sulla rete locale dell'Ente camerale, affinché siano regolarmente sottoposti alle procedure di *backup*.

8.6 L'*assegnatario* della postazione mobile è unico responsabile per l'uso appropriato e diligente del *sistema informatico* assegnato nelle modalità di *networking*, con particolare attenzione alle attività telematiche in luoghi pubblici che consentano interconnessioni ISP (*Internet Services Provider*).

8.7 L'eventuale utilizzo della postazione con diritti di amministrazione locale da parte dell'*assegnatario* deve essere preventivamente concordato con l'Ufficio Sistemi Informatici.

8.8 L'eventuale installazione di *software* aggiuntivo sulla postazione mobile da parte dell'*assegnatario* presuppone diritti di amministrazione locale adeguati e deve essere concordato con l'Ufficio Sistemi Informatici che, valutandone l'opportunità tecnica e di sicurezza, provvederà ad aggiornare e condividere la scheda di assegnazione di cui al precedente punto 8.1.

8.9 Valgono per le attrezzature informatiche mobili le disposizioni previste ai precedenti punti 6.5, 6.6, 6.7 e 6.8 del presente Capo.

9. Modalità di aggiornamento del sito *web*

9.1 L'inserimento e l'aggiornamento dei dati sui siti *web* della Camera di Commercio avviene tramite uno strumento *software* che consente a ciascuna unità organizzativa l'autonoma gestione dei contenuti (*CMS*) delle pagine e sezioni di propria competenza.

9.2 L'aggiornamento delle pagine del sito è eseguito dai referenti informatici autorizzati seguendo le indicazioni del Direttore d'ufficio competente e la procedura informatica approntata dall'Ente camerale.

9.3 I dati inseriti nelle pagine *web* di rispettiva competenza dovranno essere preventivamente sottoposti al vaglio del Dirigente dell'Area che, nella sua qualità di Responsabile del trattamento, sentito il Direttore d'ufficio dell'unità organizzativa interessata, ne autorizzerà la pubblicazione.

Titolo II
Posta elettronica

10. Finalità di utilizzo

10.1 L'osservanza delle disposizioni di cui al presente Titolo costituisce condizione essenziale per l'attribuzione in uso al dipendente di una casella e-mail da parte dell'Amministrazione camerale.

10.2 Il dipendente ha il dovere di utilizzare la Posta elettronica per finalità legittime, in stretta connessione allo svolgimento delle proprie mansioni, e quindi esclusivamente per eseguire attività istituzionali ufficiali e per effettuare comunicazioni correlate alle funzioni della Camera di Commercio.

10.3 E' vietato, salvo quanto previsto al Titolo IV del presente Capo, l'utilizzo della posta elettronica per ragioni personali estranee al servizio.

10.4 L'Ente camerale fornisce anche caselle di posta elettronica c.d. "di struttura", ossia indirizzi di posta condivisi che permettono sia la ricezione che l'inoltro della posta a gruppi di soggetti, tipicamente legate ad un ufficio o servizio. Tali caselle devono essere utilizzate per le comunicazioni che riguardano l'intera unità organizzativa alla quale si riferiscono e devono essere gestite dai dipendenti con le stesse modalità stabilite per la casella nominativa.

11. Modalità di utilizzo

11.1 Gli utenti di *account* di posta sono responsabili in via esclusiva del contenuto di messaggi, *file* di testo, immagini, *file* audio da essi trasmessi attraverso il sistema di posta elettronica della Camera di Commercio.

11.2 In particolare, in relazione all'utilizzo della posta elettronica, i dipendenti devono:

a) evitare di rivelare informazioni confidenziali;

b) evitare di rappresentare la posizione dell'Ente camerale riguardo a qualsiasi questione di carattere pubblico, salvo per l'esecuzione di attività di natura professionale autorizzata;

c) porre in essere ogni sforzo per salvaguardare l'immagine pubblica dell'Ente camerale;

d) non divulgare, né rispondere o inoltrare messaggi di natura ripetitiva (esempio: catene di S. Antonio), anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazione di virus); il dipendente, in tal caso, dovrà limitarsi ad eliminare tali messaggi e ad inoltrare un avviso all'indirizzo di posta elettronica istituzionale: info@tn.camcom.it;

e) fare attenzione agli allegati di posta elettronica provenienti da mittenti non conosciuti che potrebbero contenere dei virus.

11.3 Per tutelare la sicurezza della rete camerale, l'Ente camerale, per il tramite dell'*Amministratore di sistema*, può disporre l'introduzione di funzioni che limitano il traffico di messaggi di posta elettronica (quote spazio disco, dimensione massima degli allegati, etc.).

11.4 In caso di assenza programmata, il dipendente deve utilizzare l'apposita funzionalità automatica di avviso al mittente dell'assenza del destinatario contenente le "coordinate" elettroniche e telefoniche di un soggetto sostituto indicato dal Direttore dell'ufficio di appartenenza. Le modalità di impostazione del sistema di risposta "fuori sede" sono esemplificate nell'Allegato n. 5.

11.5 L'Ente camerale, nel caso di cessazione del rapporto di lavoro, si riserva il diritto di accedere alla posta presente sul relativo *account* e di trattenere copia dei messaggi che risultino necessari a garantire la continuità dei rapporti dell'Ente camerale con i

terzi. A tal fine, il dipendente dimissionario o quiescente deve dichiarare, tramite apposito modulo, di aver conservato all'interno della propria casella di posta solo i messaggi contenenti informazioni e documenti rilevanti per l'attività lavorativa dell'unità organizzativa a cui apparteneva (cfr. Allegato n. 2).

Titolo III
Internet

12. Finalità di utilizzo

12.1 L'osservanza delle seguenti disposizioni è condizione essenziale per l'abilitazione del dipendente al servizio di accesso a Internet da parte dell'Ente camerale.

12.2 Gli utenti di rete hanno il dovere di utilizzare la rete Internet per finalità legittime ed eticamente corrette, in stretta connessione allo svolgimento delle proprie mansioni e per attività autorizzate svolte nell'interesse dell'Ente camerale.

12.3 E' consentito l'accesso ai siti *web* e alla intranet camerale gestiti direttamente ed ospitati dall'infrastruttura informatica interna dell'Ente camerale, per i quali non è necessario un accesso alla rete Internet.

12.4 E' vietato, salvo quanto previsto al Titolo IV del presente Capo, l'utilizzo di Internet per ragioni personali estranee al servizio.

13. Modalità di utilizzo

13.1 Gli utenti di rete sono responsabili in via esclusiva del contenuto di messaggi, documenti di testo, immagini e *file* multimediali da essi pubblicati o trasmessi attraverso la rete Internet ed intranet.

13.2 In particolare, in relazione all'utilizzo della rete Internet, i dipendenti devono:

a) evitare la rivelazione di informazioni confidenziali;

b) evitare di rappresentare, se non espressamente autorizzati, la posizione della Camera di Commercio riguardo qualsiasi questione di carattere pubblico in occasione della partecipazione a news-group, *forum* pubblici o gruppi di discussione;

c) porre in essere ogni sforzo per salvaguardare l'immagine pubblica dell'Ente camerale.

Titolo IV
Criteri e modalità di utilizzo personale del sistema informativo camerale

14. Criteri di utilizzo personale

14.1 In deroga ai predetti divieti, è ammesso l'utilizzo personale dei servizi di Internet e di posta elettronica nonché delle attrezzature informatiche al fine di consentire ai dipendenti di assolvere incombenze amministrative e burocratiche senza allontanarsi dai luoghi di lavoro (ad esempio, per effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di pubblici servizi), in linea con quanto prevede la Direttiva nr. 02/09 dd. 26.05.2009 del Ministro per la Pubblica amministrazione e l'Innovazione; limitatamente a tali operazioni è consentita, in deroga al vigente divieto, la stampa dei documenti strettamente necessari.

15. Modalità dell'utilizzo personale

15.1 L'utilizzo personale di Internet, della posta elettronica e, laddove consentito, delle attrezzature informatiche deve avvenire in conformità delle disposizioni contenute nel presente Disciplinare e, in particolare, nel rispetto dei seguenti principi:

a) assenza di aggravio diretto di spesa per l'Amministrazione;
b) assenza di interferenza con i tempi di lavoro condivisi con colleghi e collaboratori;
c) puntuale rispetto delle disposizioni sulla sicurezza e la protezione dei dati personali previste dal presente Disciplinare e dalle vigenti Linee Guida per la sicurezza nel trattamento dei dati personali.

15.2 Nell'ambito dell'uso personale dei servizi e delle attrezzature informatiche, non sono comunque consentite le attività che interferiscono con l'efficienza e le funzionalità dei sistemi informatici e dei servizi di rete o che necessitano di attività di assistenza e manutenzione tecnica. E' in particolare vietato/a:

a) scaricare (*download*) da Internet *file* estranei all'attività di servizio (es.: *file* audio o video), di dimensioni tali da interferire con l'efficienza dei servizi di rete o condividere gli stessi attraverso sistemi di tipo *peer to peer*; in deroga a tale divieto, è ammesso lo scarico di *file* di dimensioni ridotte, a condizione che ogni eventuale memorizzazione avvenga su supporti non di proprietà dell'Ente camerale e in condizioni di massima sicurezza (cd rom; *chiavetta USB*, etc.);
b) effettuare il *download* di *software* dalla rete Internet senza specifica autorizzazione da parte dell'*Amministratore di sistema*; tutti i *download* di *software* dovranno essere eseguiti dai referenti informatici (Antenne informatiche) espressamente autorizzati dall'*Amministratore di sistema*;
c) ogni attività anche non riconducibile al punto precedente che porti comunque alla violazione di diritti protetti dalle norme sulla proprietà intellettuale; la mancata osservanza del diritto d'autore o di accordi di licenza comporta per il trasgressore responsabilità disciplinare e responsabilità personale, a fronte di azioni legali da parte dei legittimi titolari del diritto d'autore violato;
d) collegarsi ai *canali IRC* (Internet Relay *Chat*) o attivare servizi di condivisione *file* (tipicamente P2P-*Peer to Peer* o similari);
e) produrre siti *web*, installare *web* camera, operare servizio di *hosting*, come anche la mera conservazione di *file* su supporti di proprietà dell'Ente camerale;
f) l'invio di messaggi con allegati di dimensione tale da compromettere la normale operatività della posta per l'inoltro di messaggi non sollecitati ("lettere a catena");
g) la ricerca, trasmissione o ricezione deliberata di contenuti di tipo pornografico, denigratori, diffamatori, osceni, offensivi o di istigazione all'odio razziale e all'intolleranza politico-religiosa o comunque di carattere illecito;
h) l'utilizzo delle attrezzature e dei servizi informatici per il perseguimento di scopi di profitto personale, ovvero per curare affari estranei all'attività dell'Ente camerale, sollecitare o acquisire adesioni per finalità commerciali, di propaganda in favore di organizzazioni esterne;
i) ogni altra attività di carattere illecito.

Titolo V
Trattamento dei dati, controlli, sanzioni e altre misure di tutela

16. Dati oggetto di trattamento e relativa conservazione

16.1 I dati relativi al traffico di posta elettronica vengono gestiti:
- dalla Camera di Commercio, per tutta la posta elettronica sia interna che via internet. Il contenuto delle informazioni tracciate, la modalità ed il periodo di conservazione e cancellazione delle stesse vengono effettuate nel rispetto dei termini necessari a garantire la corretta funzionalità del sistema informatico (cfr. Allegato n. 6, lett. A);
- da InfoCamere, per la sola posta elettronica via internet ad esclusione delle informazioni riguardanti specificatamente i riferimenti personali alle caselle di posta elettronica interne. Il contenuto delle informazioni tracciate, la modalità ed il periodo di conservazione e cancellazione delle stesse vengono effettuate da InfoCamere nel rispetto dei termini dichiarati dalla stessa InfoCamere "conformi dalla normativa vigente" (cfr. Allegato n. 6, lett. B).

16.2 La gestione dei dati relativi al traffico internet della Camera di Commercio, ivi compreso l'accesso e la conservazione, è interamente effettuata dalla società InfoCamere – Società consortile di informatica delle Camere di Commercio italiane per azioni. Il contenuto delle informazioni tracciate, la modalità ed il periodo di conservazione e cancellazione delle stesse vengono effettuate da InfoCamere nel rispetto dei termini dichiarati dalla stessa InfoCamere "conformi alla normativa vigente" (cfr. Allegato n. 6 lett. B).

16.3 I dati relativi alle stampe inviate alle stampanti multifunzione sono potenzialmente accessibili agli Amministratori di Sistema in relazione a interventi di assistenza informatica e manutenzione, al personale del Servizio Acquisti e Gestione in fase di verifica dei consumi delle stampanti stesse e alle Antenne informatiche nel corso della procedura di abilitazione dei colleghi all'uso delle stampanti medesime. I soggetti autorizzati al trattamento di tali dati sono vincolati all'obbligo di riservatezza richiamato nelle rispettive nomine a Incaricati del trattamento.

17. Controlli

17.1 Ai sensi e per gli effetti delle vigenti disposizioni normative in materia di privacy, l'Ente camerale è obbligato ad effettuare periodicamente controlli a garanzia della sicurezza e riservatezza dei dati personali oggetto di trattamento connesso all'utilizzo dei sistemi informatici, nel rispetto dei principi di pertinenza e non eccedenza, in osservanza delle prescrizioni di legge, con particolare riguardo agli artt. 4 e 8 della Legge 20 maggio 1970, n. 300 "Statuto dei lavoratori", nonché all'art. 24 della Legge 29 marzo 1983, n. 93 "Legge quadro sul pubblico impiego" e delle indicazioni fornite dall'Autorità garante con deliberazione 1 marzo 2007 nr. 13.

17.2 E' in ogni caso vietata ogni attività finalizzata al monitoraggio automatizzato e continuativo delle attività del lavoratore. In particolare non è consentito effettuare controlli con le seguenti finalità:
a) lettura sistematica dei messaggi di posta elettronica dei dipendenti per gestire il servizio di posta elettronica;
b) riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal dipendente;
c) lettura e registrazione sistematica dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto;
d) analisi occulta degli accessi a internet o dell'uso della posta elettronica.

17.3 Preposto alla funzione di controllo di cui al punto 17.1 è il Segretario Generale, Responsabile Privacy dell'Ente camerale, che si avvale per la concreta attuazione dei controlli prescritti della collaborazione dei Responsabili interni del trattamento dei dati, dei Responsabili di U.O. e dell'ausilio tecnico degli Amministratori di sistema.

18. Modalità di controllo

18.1 Al fine di assicurare la funzionalità, la sicurezza e il corretto impiego degli strumenti informatici e delle reti telematiche da parte degli utilizzatori, l'Amministrazione camerale, anche con il tramite di InfoCamere per i servizi descritti al precedente punto 16, si riserva di effettuare i necessari controlli, nel rispetto delle prescrizioni di cui al precedente punto 17:
- sugli accessi ad Internet;
- sulla posta elettronica ricevuta ed inviata dal dipendente, considerato che la casella di posta assegnata dall'Amministrazione all'*utente* è uno strumento di lavoro, per cui la posta ricevuta e trasmessa non è in ogni caso da considerarsi corrispondenza privata nemmeno quando i messaggi riportino la dicitura "riservato";
- sul corretto utilizzo delle attrezzature informatiche;
- sulla singola postazione di lavoro con le modalità di cui al seguente punto 18.3.

18.2 I controlli avvengono secondo le seguenti modalità:

a) controllo in forma anonima, anche automatica e a campione (c.d. controllo generale e routinario), in modo da precludere l'identificazione degli utenti e/o delle loro attività, con cadenza periodica (di norma trimestrale).
I dati anonimi aggregati, riferibili all'intera struttura, sono posti a disposizione dell'Ufficio Risorse Umane, competente in materia disciplinare, per le conseguenti valutazioni e riguardano i dati indicati al precedente punto 16 e precisamente:
   - per ciascun sito/dominio visitato: il numero di utenti che lo visitano, il numero delle pagine richieste e la quantità di dati scaricati;
   - per ciascun *utente*, presentato in forma anonima: il numero dei siti visitati, la durata del collegamento e la quantità totale dei dati scaricati.

   In caso di rilevazione di comportamenti anomali non rientranti nelle fattispecie di cui alla successiva lettera b), i dipendenti sono avvisati dell'accertato utilizzo improprio della rete Internet e contestualmente invitati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

b) controllo in forma non anonima (c.d. controllo specifico e mirato), in relazione:
   - al caso in cui l'integrità del sistema sia minata da un problema di sicurezza e sia indispensabile la consultazione dei *file* di *log* per individuare ed eliminare l'anomalia;
   - alla prevenzione e all'accertamento, in presenza di indizi, di illeciti civili, penali e amministrativi;
   - all'indispensabilità dei dati di *log* rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
   - all'obbligo di rispondere ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria;
   - al caso di persistente utilizzo anomalo degli strumenti da parte degli utenti, rilevabile esclusivamente dai dati aggregati, nonostante l'avviso a cessare tale comportamento di cui alla precedente lettera a);

18.3 Il controllo sulla singola postazione di lavoro può essere esercitato, nelle fattispecie di cui alla lettera b) del precedente punto, e laddove necessario, anche attraverso ispezioni dirette dal Segretario Generale o suo delegato e condotte d'ufficio o su

richiesta del Dirigente dell'Area di appartenenza del dipendente, eventualmente assistito dall'*Amministratore di sistema* anche ai fini del *reset* della password e alla presenza dell'*assegnatario* della postazione o suo delegato o, se impossibile, del Responsabile dell'unità organizzativa. Dell'ispezione viene redatto verbale consegnato in copia all'interessato che può rendere nel medesimo, se presente, proprie osservazioni. Nel corso dell'ispezione, il dipendente ha l'obbligo di osservare le istruzioni impartite dal Responsabile dell'ispezione medesima e di fornire la password per l'accesso al sistema (cfr. Allegato n. 7).

18.4 Le verifiche e le ispezioni sono condotte rispettivamente, su motivata richiesta:
a) dal Presidente della Camera di Commercio, per il Segretario Generale;
b) dal Segretario Generale, Capo del personale, per gli altri dipendenti.

18.5 Laddove il controllo possa compromettere il segreto professionale cui il dipendente sia chiamato per specifica norma di legge, sulla relativa opposizione decide, assunta cognizione dell'oggetto, il Segretario Generale sentito il Dirigente dell'Area di assegnazione. Nel frattempo il controllo resta sospeso. Il Segretario Generale dispone, ove necessario, le opportune misure cautelari.

18.6 Tali informazioni potranno essere comunicate solo ed esclusivamente a soggetti interni o esterni all'Ente camerale rispetto ai quali la comunicazione risulti necessaria in relazione alle finalità legittime perseguite con l'accesso.

18.7 Nell'espletare i controlli e le verifiche, gli Amministratori di sistema incaricati dall'Ente camerale devono garantire la massima riservatezza dei dati di cui siano venuti a conoscenza, anche incidentalmente, in occasione della verifica, pena l'applicazione delle sanzioni disciplinari previste dal contratto di lavoro.

18.8 Fermo restando quanto disposto al punto 1.3 del presente Disciplinare e salvo diversa previsione dei contratti collettivi, è in ogni caso fatto divieto di utilizzo dei sistemi e dei dati indicati al punto 16 ai fini della valutazione quantitativa e qualitativa della prestazione del lavoratore, nonché ai fini dell'accertamento del rispetto degli obblighi di comportamento del lavoratore nell'esecuzione del contratto di lavoro estranei all'ambito di regolazione del presente disciplinare e sempre che il comportamento non costituisca diverso illecito civile, penale e amministrativo.

19. Sanzioni e altre misure di tutela

19.1 Salvo quanto previsto al precedente punto 18.8, l'accertato mancato rispetto dei predetti divieti, obblighi e prescrizioni è punito secondo quanto previsto dal Codice disciplinare, ferme restando, in capo al dipendente, le ulteriori responsabilità in sede civile, penale e amministrativa.

19.2 L'utilizzo del servizio di accesso ad Internet e della posta elettronica può essere sospeso o interrotto d'ufficio nei seguenti casi:
a) qualora non sussista più la condizione di dipendente o collaboratore autorizzati o non fosse confermata l'autorizzazione all'uso;
b) qualora venga accertato un uso non corretto del servizio da parte dell'*utente* o comunque un uso incompatibile con i suoi compiti professionali;
c) in caso di manomissioni e/o interventi sul *hardware* e/o sul *software* impiegati per la connessione compiuti dall'*utente* a ciò non autorizzato;
d) in caso di diffusione o comunicazione, imputabili direttamente o indirettamente all'*utente*, di password, procedure di connessione, *indirizzo IP* ed altre informazioni tecniche riservate;
e) in caso di accesso doloso dell'*utente* a *directory*, siti, *file* e servizi da chiunque resi disponibili e, in ogni caso, qualora l'attività dell'*utente* comporti danno, anche solo potenziale, al sito contattato;

f) in ogni altro caso in cui sussistano ragionevoli evidenze di una violazione degli obblighi dell'*utente*.

Titolo VI
Misure di garanzia

20. Misure organizzative

20.1 Al fine di assicurare la funzionalità, la sicurezza e il corretto impiego degli strumenti informatici e delle reti telematiche da parte degli utilizzatori, l'Amministrazione camerale, attraverso le strutture competenti, garantisce le seguenti misure organizzative:

a) sistematica valutazione degli effetti sui diritti dei lavoratori prodotti dall'introduzione e applicazione di nuove misure volte a salvaguardare la sicurezza ed il mantenimento dell'efficienza dei sistemi;
b) individuazione (anche tipologica) dei lavoratori cui è accordato l'utilizzo della posta elettronica e internet. L'assegnazione al dipendente delle dotazioni strumentali d'ufficio, ivi compresi i diversi applicativi quali internet, posta elettronica, banche dati, *software* specialistici, nonché le relative abilitazioni, è richiesta dal Responsabile di U.O. in riferimento alle mansioni svolte dal dipendente tramite l'utilizzo dell'apposita scheda informatica esemplificata nell'Allegato n. 1;
c) ubicazione dei *server* in apposite stanze a ciò destinate o in armadi chiusi muniti di serratura e/o altre protezioni adeguate con relativa individuazione dell'incaricato alla custodia;
d) accessibilità delle postazioni di lavoro solo a quanti ne hanno titolo, in qualità di Responsabili o Incaricati del trattamento o Amministratori di sistema, nei soli limiti in cui ciò sia funzionale allo svolgimento dei compiti della struttura o per lo svolgimento di attività di manutenzione, di pulizia e affini, nonché per altre attività comunque indispensabili;
e) accesso fisico ai luoghi di lavoro protetto tramite la presenza di personale addetto ai servizi ausiliari ovvero tramite la chiusura delle vie di accesso, sempre nel rispetto delle norme antincendio;
f) presidio del personale addetto ai servizi ausiliari degli uffici aperti al pubblico; negli orari diversi da quelli di servizio, ove non vi sia comunque un presidio, la porta di accesso all'edificio deve rimanere chiusa;
g) presenza di dipendenti abilitati quali "*Amministratore di sistema*" a sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e a consentirne l'utilizzazione. In caso di assenza dell'Incaricato al trattamento che non possa avvalersi del servizio di web mail o non sia raggiungibile e di urgenza di accesso ai dati, ivi compresi quelli contenuti nella posta elettronica, l'*Amministratore di sistema*, su richiesta scritta e motivata del Dirigente responsabile, consente l'accesso ai dati al Direttore d'Ufficio competente tramite il *reset* della password del dipendente assente. L'uso della password è infatti da intendersi unicamente come strumento di protezione da accessi non autorizzati dall'Amministrazione. Dell'avvenuto accesso è data comunicazione al dipendente (cfr. Allegato n. 8);
h) l'Amministrazione impegna gli Amministratori di sistema, in piena conformità alla normativa vigente ivi comprese le presenti disposizioni, a garantire il segreto sugli atti e le informazioni di cui gli stessi vengano a conoscenza, ad adottare le misure necessarie ad assicurare che i controlli avvengano nei limiti sopra definiti nonché a ridurre le operazioni di manutenzione allo stretto necessario. A questo scopo, gli Amministratori di sistema sono destinatari di corsi di formazione organizzati

periodicamente dall'Amministrazione camerale sulla gestione e sulla sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto delle comunicazioni.

21. Misure tecnologiche

21.1 Per le stesse finalità di cui al punto 20.1, l'Ente camerale adotta le seguenti misure tecnologiche rispetto alla navigazione Internet:

a) protezione della rete con *firewall*, gestito dalla società InfoCamere;
b) accesso alla postazione informatica e alla rete attraverso l'utilizzo di un identificativo *utente* (user-id) e di una password;
c) periodica sostituzione della password su richiesta del sistema;
d) *screen saver* vincolato e automatico protetto da password con tempo di attivazione automatico;
e) adozione di sistemi e di filtri gestiti dalla società InfoCamere volti a prevenire determinate operazioni vietate quali ad esempio un sistema di "*url filtering*" per il monitoraggio del traffico *web* che permette di bloccare la navigazione verso i principali siti non consentiti conosciuti, contenenti materiale per soli adulti o riconducibili a pratiche illecite (cfr. Allegato n. 6, lett. C.);
f) trattamento delle registrazioni in forma anonima o tale da precludere l'immediata identificazione degli utenti, mediante opportune aggregazioni;
g) in caso di conservazione delle registrazioni, limitazione al tempo strettamente necessario al perseguimento delle finalità organizzative, produttive e di sicurezza, attraverso procedure di cancellazione periodica automatica (sovraregistrazione) dei dati personali relativi agli accessi ad Internet e al traffico telematico, salvo i casi di particolari esigenze di sicurezza, difesa in sede giudiziaria e ragioni di giustizia;
h) i controlli sui comportamenti anomali, esclusi in ogni caso quelli prolungati, costanti ed indiscriminati, sono graduati secondo le modalità previste al precedente punto 18.

21.2 Per le stesse finalità di cui al punto 20.1, l'Ente camerale adotta le seguenti misure tecnologiche rispetto alla posta elettronica:

a) eventuale attivazione di caselle c.d. "di struttura", ossia indirizzi di posta condivisi che permettono sia la ricezione che l'inoltro della posta a più soggetti purché preventivamente e adeguatamente autorizzati;
b) invito a tutti gli utenti a configurare dal proprio *client* di posta elettronica, nel caso di assenza programmata, un messaggio di risposta automatica, che indichi i riferimenti elettronici e/o telefonici di altro referente dell'ufficio e/o struttura di appartenenza;
c) possibilità da parte del Responsabile del trattamento (Dirigente), su richiesta del Direttore d'Ufficio competente, qualora il lavoratore sia irreperibile o non possa attivare la procedura "fuori sede" descritta anche avvalendosi del servizio di *web*-mail e ne sussista la necessità, di disporre lecitamente, avvertendone al suo rientro l'interessato e avvalendosi della collaborazione tecnica dell'*Amministratore di sistema*, l'attivazione di un analogo accorgimento;
d) possibilità da parte del Responsabile del trattamento (Dirigente) - qualora si presenti la necessità, per improrogabili ragioni di ufficio, di accedere ai dati contenuti in una casella di posta elettronica e l'Incaricato abilitato all'accesso a tale casella sia irreperibile o non possa avvalersi del servizio di web-mail - di chiedere all'*Amministratore di sistema* il *reset* della password e disporre l'accesso a tale casella da parte del Direttore d'ufficio competente;
e) con procedura automatica i messaggi di posta elettronica riportano un avvertimento ai destinatari nel quale sia dichiarato, da un lato, il carattere confidenziale delle informazioni contenute nel messaggio rispetto ai destinatari dello stesso e, dall'altro,

la natura non riservata della corrispondenza stante la possibilità che la risposta sia letta da altri soggetti incaricati appartenenti all'Ente camerale (cfr. Allegato n. 9);

f) i controlli sui comportamenti anomali sono graduati secondo le modalità previste al precedente punto 18.

CAPO III
FORMAZIONE A DISTANZA (FAD)

22. Finalità di utilizzo

22.1 Le informazioni personali relative al traffico FAD vengono trattate per realizzare e gestire le iniziative formative, con conseguente valutazione e certificazione della partecipazione, per l'elaborazione di statistiche e per il compimento di operazioni connesse al miglioramento del sistema.

22.2 Le informazioni di cui al precedente punto 22.1 sono detenute dall'Ente formatore al fine di consentire lo svolgimento della funzione istituzionale inerente la formazione, lo sviluppo e l'aggiornamento dei dipendenti camerali.

23. Misure organizzative

23.1 I soggetti che, a diverso titolo, assumono ruoli di responsabilità, direttivi e operativi nel trattamento dei dati personali di cui al precedente punto sono così individuati:

a) Titolare del trattamento: Camera di Commercio I.A.A. di Trento;
b) Responsabile del trattamento: Ente formatore;
c) *Amministratore di sistema* individuato dall'Ente formatore;
d) Incaricati del trattamento: soggetti autorizzati dal Responsabile del trattamento, tra cui i docenti dell'iniziativa formativa;

23.2 Il Dirigente è responsabile, nell'espletamento dei propri compiti di organizzazione e gestione del personale assegnato, del trattamento dei dati personali relativi all'individuazione dei dipendenti che partecipano alle iniziative formative.

23.3 I soggetti di cui al primo comma del presente articolo dovranno attenersi alle direttive esecutive in applicazione del D.Lgs. 196/2003 e s.m.i. (Codice in materia di protezione dei dati personali).

24. Dati oggetto del trattamento relativi alla FAD e relativa conservazione

24.1 I dati oggetto del trattamento si distinguono a seconda che siano fruibili dai ruoli Amministratore, Docente ed E-Tutor, ovvero dai singoli Partecipanti al corso.

24.2 Il trattamento di dati relativi al ruolo Amministratore – Docente – E-Tutor riguarda:

1) anagrafica personale (nome/cognome/e-mail/matricola/codice fiscale);
2) anagrafica dei partecipanti al corso;
3) iscrizione al corso;
4) ultimo accesso al corso;
5) tempo trascorso su un materiale didattico;
6) altre statistiche *SCORM*: numero di accessi ad un determinato oggetto didattico (numero play), percentuale di completamento del corso (tempo di fruizione e completamento del materiale);
7) statistiche relative a: questionari (risposta alla singola domanda), risultato test di valutazione;
8) utilizzo di servizi all'interno della comunità del corso (tempo e periodo d'uso: mese/settimana/giornata);
9) tempo trascorso all'interno dell'applicativo del corso;

10) presenza on line del Partecipante.

24.3 Il trattamento di dati relativi al ruolo Partecipante al corso riguarda:
1) anagrafica personale (nome/cognome/e-mail/matricola/codice fiscale);
2) iscrizione al corso;
3) ultimo accesso al corso;
4) tempo trascorso su un materiale didattico;
5) altre statistiche *SCORM*: numero di accessi ad un determinato oggetto didattico (numero play), percentuale di completamento del corso (tempo di fruizione e completamento del materiale);
6) statistiche relative a: questionari (risposta alla singola domanda), risultato test di valutazione;
7) utilizzo di servizi all'interno della comunità del corso (tempo e periodo d'uso: mese/settimana/giornata);
8) tempo trascorso all'interno dell'applicativo del corso.

24.4 I partecipanti al corso possono visionare le proprie attività con esclusione di quelle degli altri partecipanti ad eccezione delle attività che prevedono interazioni fra gli stessi quali le funzionalità di *chat*, *forum*, *wiki* o *quaderno condiviso*, che permettono ad un *utente* di mettere a disposizione degli altri partecipanti proprie elaborazioni o documenti di propria scelta/produzione. I dati personali esposti da queste funzionalità sono il nome/cognome di chi condivide, accompagnati dalla data di inserimento dell'attività (conversazione per il *chat*, il *post* per il *forum*, l'*upload* per il quaderno, etc.).

24.5 I sistemi informativi ed i programmi informatici sono configurati, soprattutto nel caso di effettuazione di analisi quali-quantitative o statistiche anche temporali, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi, anche avuto riguardo agli obbiettivi didattici, possono essere realizzate mediante dati anonimi o opportune modalità che permettano di identificare l'interessato solo in caso di necessità (art. 3 D.Lgs. 196/2003).

24.6 Fatto salvo quanto previsto in materia di certificazione sulla partecipazione, va in ogni caso preferito il trattamento di dati anonimi (principio di pertinenza) e con modalità tali da determinare il minimo sacrificio possibile del diritto alla riservatezza (principio di non eccedenza) con particolare riguardo ai dati sub n. 5), 6), 7), 8), 9) e 10) del ruolo Amministratore – Docente – E-Tutor.

24.7 Il traffico FAD è conservato presso i *server* gestiti dagli Amministratori di Sistema indicati dall'Ente formatore.

24.8 I dati della formazione a distanza sono conservati per l'intera durata del relativo progetto.

25. Modalità di fruizione da parte dei dipendenti camerali

25.1 Le modalità di fruizione dei corsi in modalità FAD dovranno avvenire secondo la procedura prevista nell'Allegato n. 10.

26. Certificazione sulla partecipazione

26.1 La certificazione dei corsi in modalità FAD viene rilasciata dal gestore del corso tenuto conto dei dati anagrafici, di iscrizione e di accesso al corso e, per il fatto che la presenza in FAD è virtuale, del completamento delle attività on line da parte del partecipante e del tempo trascorso all'interno del corso, prevedendo – laddove compatibile con l'obiettivo didattico – il positivo superamento di una verifica finale in aula ovvero on line con metodologie che garantiscano l'identità.

27. Controlli

27.1 L'Amministrazione si riserva di effettuare i controlli per le finalità e con le modalità di cui ai punti 17 e 18 del presente Disciplinare.

CAPO IV
SERVIZI TELEFONICI

Titolo I
Regole comportamentali nell'utilizzo dei telefoni e apparecchiature fax

28. Uso dei telefoni fissi

28.1 L'Ente camerale non si rende in nessun caso responsabile per danni recati a terzi causati dall'uso scorretto delle attrezzature telefoniche da parte dell'*assegnatario*, in particolare dall'uso non conforme alle disposizioni del presente Disciplinare.

28.2 I dipendenti non possono utilizzare le linee telefoniche dell'ufficio e i mezzi di comunicazione vocale assimilabili (es.: *softphone* per effettuare chiamate tramite PC; sistemi di videochiamata/videoconferenza) per effettuare telefonate personali. Durante l'orario di lavoro la ricezione di telefonate personali sulle linee telefoniche dell'ufficio è limitata al minimo indispensabile.

28.3 In deroga a quanto disposto al punto precedente, sono ammesse brevi e limitate comunicazioni telefoniche personali:
- tra i dipendenti camerali;
- verso soggetti esterni, solo in casi eccezionali e urgenti.

28.4 In caso di assenza e laddove l'apparecchio già non sia così configurato in via automatica, è opportuno deviare il proprio numero interno sull'apparecchio di un collega, seguendo le disposizioni del Direttore d'Ufficio competente.

28.5 Salvo quanto previsto dal precedente punto 28.4, nel caso di assenza o comunque di impossibilità a rispondere, il collega d'ufficio che occupa la medesima stanza riceve le telefonate del collega, seguendo le disposizioni del Direttore d'Ufficio competente.

28.6 Eventuali guasti devono essere segnalati quanto prima all'Ufficio Economato.

29. Uso aziendale dei servizi di telefonia mobile

29.1 In relazione alle necessità connesse allo svolgimento dell'attività lavorativa, il Segretario Generale, su proposta dei responsabili delle unità operative, può assegnare a un "consegnatario" apparecchi e/o servizi di telefonia mobile o assimilabili. Gli apparecchi saranno accompagnati da una "scheda di consegna" (cfr. Allegato n. 4) e da una "scheda informativa".

29.2 Al fine di evitare un utilizzo improprio, si evidenzia che il consegnatario è il responsabile unico del corretto utilizzo degli apparati di servizio di cui dispone. Nel caso in cui un apparecchio sia concesso in uso ad un Ufficio o Servizio, pertanto a più utilizzatori, il consegnatario sarà individuato nel Direttore d'Ufficio. In tal caso, l'Ufficio o Servizio dovrà predisporre apposita scheda, annotando sulla stessa gli utilizzatori e i periodi di utilizzo.

29.3 In ogni caso, al fine di ridurre il possibile uso fraudolento nell'eventualità di furto o smarrimento, il consegnatario o l'utilizzatore deve sempre attivare la richiesta del codice di identificazione (PIN) all'accensione del cellulare.

29.4 L'uso a fini personali delle apparecchiature dell'Ente camerale può avvenire solo se è operativo il servizio *dual-billing* (doppia fatturazione), che, anteponendo il codice prescritto, permette di addebitare i costi per l'uso privato sul conto corrente personale

del consegnatario. A tal fine si fa riferimento al documento "Criteri per l'erogazione del servizio Dual Billing" consegnato al momento dell'attivazione del servizio.

29.5 In caso di furto o smarrimento degli apparati e/o delle schede sim, il consegnatario dovrà:
- chiamare immediatamente il numero verde del Customer care indicato nella "scheda informativa" di cui al punto 29.1 ed effettuare il blocco dell'utenza;
- presentare denuncia presso le autorità competenti, precisando tutti gli elementi che possono ricondurre all'utenza stessa (rintracciabili nella scheda informativa e nella scheda di consegna);
- contattare l'Ufficio Economato che provvederà, nei tempi e modi previsti dal contratto, al reintegro dell'apparato.

29.6 E' vietato l'invio dei cosiddetti SMS solidali (per le donazioni) e degli SMS premium con i quali è possibile sottoscrivere un abbonamento ad un servizio che, a sua volta, prevede l'invio periodico e automatico di messaggi a pagamento contenenti suonerie, oroscopo, ecc.

30. Uso del fax

30.1 I dipendenti non utilizzano le attrezzature fax dell'ufficio per effettuare trasmissioni di documenti personali.

30.2 In deroga a quanto disposto al punto precedente, solo in casi eccezionali e urgenti, è ammesso l'uso personale del fax.

30.3 Non devono essere lasciate incustodite le attrezzature fax in caso di invio o ricezione di atti o documenti il cui contenuto possa venire a conoscenza di soggetti non autorizzati al trattamento dei dati in essi contenuti.

30.4 Nelle note inviate a mezzo fax va inserita sempre la copertina riportante la dicitura indicata nell'Allegato n. 9 al presente disciplinare.

Titolo II
Dati oggetto di trattamento, controlli, sanzioni e altre misure di tutela

31. Conservazione dei dati telefonici

31.1 Il fornitore dei servizi telefonici conserva i dati di traffico telefonico nel rispetto di quanto previsto dal provvedimento a carattere generale del Garante per la protezione dei dati personali datato 17 gennaio 2008 e s.m.i. avente ad oggetto "Sicurezza dei dati di traffico telefonico e telematico".

31.2 Ai sensi dell'art. 124 del D.Lgs. 196/2003, nella fatturazione dell'abbonato non sono evidenziate le ultime tre cifre dei numeri chiamati. Ad esclusivi fini di specifica contestazione dell'esattezza di addebiti determinati o riferiti a periodi limitati, l'abbonato può richiedere la comunicazione dei numeri completi delle comunicazioni in questione.

32. Controlli sui dati telefonici

32.1 I controlli sui dati telefonici possono essere:

a) in forma anonima, anche a campione e automatici, sui telefoni fissi: il Dirigente dell'Area 2 - Amministrazione trasmette ai Direttori d'Ufficio i dati relativi al superamento per ogni bimestre della percentuale massima di tolleranza, c.d. "soglia", determinata dall'incremento superiore al 20% dell'importo fatturato rispetto al corrispondente bimestre dell'anno precedente, chiedendo informazioni a riguardo. I dipendenti assegnati ai/l Servizio/i coinvolto/i saranno genericamente richiamati dal Direttore di riferimento al corretto utilizzo del telefono, nel rispetto delle disposizioni

del vigente disciplinare; sono equiparati al trattamento dei dati in forma anonima anche i dati di ogni singola utenza ma aggregati per direttrice (es.: SMS, *roaming* internazionali, off net, ecc.) non evidenziati in tabulati analitici;

b) in forma non anonima "c.d. controllo specifico e mirato", sui telefoni fissi e sui cellulari di servizio, in base a tabulati analitici e in relazione:
   - al caso in cui l'integrità delle linee telefoniche sia minata da un problema di sicurezza;
   - alla prevenzione e all'accertamento, in presenza di indizi, di illeciti civili, penali e amministrativi;
   - a fatturazioni che laddove dettagliate – perché "sospette" – evidenzino un utilizzo improprio del cellulare di servizio (es.: loghi e suonerie; da concorsi e sondaggi, etc.); in questo caso l'identificazione dell'*utente* è coessenziale al controllo che, pertanto, sarà sempre e solo in forma non anonima;
   - all'indispensabilità dei dati di *log* rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
   - all'obbligo di rispondere ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria;
   - al caso di persistente utilizzo anomalo degli strumenti da parte degli utenti di una specifica struttura/area (rilevabile esclusivamente dai dati aggregati), nonostante l'avviso a cessare tale comportamento.

32.2 Tali controlli puntuali sono ammessi su motivata richiesta:
a) del Presidente della Camera di Commercio, per il Segretario Generale;
b) del Segretario Generale, Capo del personale, per gli altri dipendenti.

32.3 Laddove il controllo possa compromettere il segreto professionale cui il dipendente sia chiamato per specifica norma di legge, sulla relativa opposizione decide, assunta cognizione dell'oggetto, il Segretario Generale sentito il Dirigente dell'Area di assegnazione. Nel frattempo il controllo resta sospeso. Il Segretario Generale dispone, ove necessario, le opportune misure cautelari.

32.4 Fermo restando quanto disposto al precedente punto 1.3 del presente Disciplinare e salvo diversa previsione dei contratti collettivi, è in ogni caso fatto divieto di utilizzo dei sistemi e dei dati indicati al precedente punto 32.1 ai fini della valutazione quantitativa e qualitativa della prestazione del lavoratore, nonché ai fini dell'accertamento del rispetto degli obblighi di comportamento del lavoratore nell'esecuzione del contratto di lavoro estranei all'ambito di regolazione del presente disciplinare e sempre che il comportamento non costituisca diverso illecito civile, penale e amministrativo.

33. Sanzioni e altre misure di tutela

33.1 Salvo quanto previsto al precedente punto 32.4, l'accertato mancato rispetto dei predetti divieti, obblighi e prescrizioni è punito secondo quanto previsto dal Codice disciplinare, ferme restando, in capo al dipendente, le ulteriori responsabilità in sede civile, penale e amministrativa;

33.2 In ogni caso in cui sussistano ragionevoli evidenze di una violazione degli obblighi dell'*utente*, può essere disposta la sospensione o la revoca del servizio telefonico (fisso e/o mobile) ovvero può essere limitato il servizio di accesso alla rete telefonica.

CAPO V
DISPOSIZIONI FINALI

34. Pubblicità ed entrata in vigore

34.1 Il presente Disciplinare è pubblicato all'Albo della Camera di Commercio I.A.A. di Trento per otto giorni consecutivi ed entra in vigore il primo giorno successivo dal termine della pubblicazione. Copia del disciplinare verrà trasmessa via posta elettronica a tutti i dipendenti camerali.

35. Informativa ai lavoratori ai sensi dell'art. 13, D.Lgs. n. 196/2003

35.1 Si rinvia in merito all'*Appendice A* del presente Disciplinare.

APPENDICE A Nota informativa sul trattamento dati personali relativi all'utilizzo della rete internet, della posta elettronica e delle attrezzature informatiche e telefoniche ai sensi dell'art. 13 del D. Lgs n. 196/2003 (Codice privacy).

Con riferimento al Disciplinare relativo all'utilizzo della rete internet, della posta elettronica e delle attrezzature informatiche e telefoniche, La si informa che ogni trattamento dei Suoi dati personali avverrà nei seguenti termini:

a) Oggetto del trattamento: informazioni relative al Suo utilizzo di Internet, della posta elettronica nonché delle attrezzature informatiche e telefoniche, comprensive di eventuali dati sensibili (opinioni religiose, filosofiche, politiche, stato di salute e vita sessuale);
b) Finalità del trattamento: verifica del corretto utilizzo di Internet, posta elettronica e degli strumenti informatici e telefonici a garanzia della disponibilità ed integrità dei sistemi informativi nonché della sicurezza sul lavoro;
c) Modalità del trattamento: informatizzato e manuale; effettuato da soggetti autorizzati all'assolvimento di tali compiti, edotti dei vincoli imposti dal D.Lgs. n. 196/2003 e con misure atte a garantire la riservatezza dei dati ed evitare l'accesso ai dati stessi da parte di soggetti terzi non autorizzati;
d) Obbligatorietà del conferimento dati: in quanto indispensabile per l'assolvimento delle anzidette finalità; l'opposizione al trattamento potrebbe comportare l'impossibilità della prosecuzione del rapporto;
e) Esercizio dei diritti dell'interessato di cui agli artt. 7 e 9 del D.Lgs. 196/2003: anche mediante terza persona fisica, ente, associazione od organismo cui abbia conferito delega o procura, per conoscere i dati che lo riguardano ed intervenire circa il loro trattamento.

Il TITOLARE del trattamento dei Suoi dati è la Camera di Commercio I.A.A. di Trento con sede in via Calepina, 13 – 38122 Trento.

I RESPONSABILI per il trattamento di dati personali relativi alle materie di rispettiva competenza e alle funzioni di gestione amministrativa, finanziaria e tecnica sono:

- il Segretario Generale (Responsabile Privacy);
- il Suo Dirigente di Area (Responsabile del trattamento);
- la società InfoCamere S. Cons. a r.l. (Responsabile esterno del trattamento con funzioni di *Amministratore di Sistema*);
- gli Enti per la FAD (Responsabili esterni del trattamento).

IL SEGRETARIO GENERALE
(Responsabile Privacy)

APPENDICE B - GLOSSARIO

ACCOUNT: costituisce quell'insieme di funzionalità, strumenti e contenuti attribuiti ad un *utente* in determinati contesti operativi. In informatica, attraverso il meccanismo dell'*account*, il sistema mette a disposizione dell'*utente* un ambiente con contenuti e funzionalità personalizzabili, oltre ad un conveniente grado di isolamento dalle altre utenze parallele;

AMMINISTRATORE DI SISTEMA: il soggetto a cui è conferito il compito di sovrintendere al sistema informatico e di consentirne l'utilizzazione. La prevista pubblicità dell'identità degli Amministratori di sistema è attuata nella Sezione Privacy della Intranet camerale;

ASSEGNATARIO: qualsiasi soggetto, dipendente e non, a cui venga assegnata in uso a qualunque titolo attrezzatura informatica o telefonica appartenente all'Ente camerale;

BACKUP: copia di sicurezza o copia di riserva, indica l'operazione tesa a duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di stazione di lavoro, o di un *server*. Normalmente viene svolta con una periodicità stabilita;

BYTE: è l'unità elementare di memorizzazione composta da 8 bit . Di solito un *byte* rappresenta un singolo carattere, come un numero, una lettera o un simbolo;

BLACK LIST: elenco di siti non accessibili da nessun *utente*;

BLACKBERRY: connettività wireless (dall'inglese senza fili – sistemi di comunicazione tra dispositivi elettronici, che non fanno uso di cavi), che consente di restare collegati con i propri contatti anche quando si è lontani dall'ufficio;

CANALI IRC (internet relay *chat*): il canale è il mezzo di comunicazione fondamentale in una sessione IRC, un gruppo di utenti identificato da un nome, dove tutti gli appartenenti possono mandare messaggi leggibili solo dagli utenti dello stesso gruppo;

CHAT il termine ***chat*** (in inglese, letteralmente, "chiacchierata"), viene usato per riferirsi a un'ampia gamma di servizi che hanno tutti in comune due elementi fondamentali: il fatto che il dialogo avvenga in tempo reale e il fatto che il servizio possa mettere facilmente in contatto sconosciuti, generalmente in forma anonima;

CHIAVE USB (o penna USB, o pendrive): è una memoria di massa portatile di dimensioni molto contenute (qualche centimetro in lunghezza e intorno al centimetro in larghezza) che si collega al computer mediante la comune *porta* USB ;

CLIENT: una componente che accede ai servizi o alle risorse di un'altra componente, detta *server*. In questo contesto si può quindi parlare di *client* riferendosi all'*hardware* o al *software*;

CMS : Sistema di Gestione dei Contenuti, è uno strumento software installato su un server web studiato per facilitare la gestione dei contenuti di siti web;

CREDENZIALI DI AUTENTICAZIONE: le credenziali di autenticazione (login) consistono in un codice per l'identificazione dell'incaricato (user-id) associato a una parola riservata (password) conosciuta esclusivamente dal possessore, oppure in un dispositivo di autenticazione ad uso esclusivo dell'incaricato (dispositivo di firma elettronica), ad un codice identificativo o in una caratteristica biometrica;

DIRECTORY: è una specifica entità del *file* system che elenca altre entità, tipicamente *file* e altre directory, e che permette di organizzarle in una struttura ad albero;

DISASTER RECOVERY: l'insieme di misure tecnologiche atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business a fronte di gravi emergenze.

DOWNLOAD: trasferire programmi o dati da un'unità connessa al proprio computer ad un personal computer;

FAD formazione a distanza;

FILE: un contenitore di informazione digitalizzata. Le informazioni codificate al suo interno sono leggibili solo da *software*;

FIREWALL: apparato di rete *hardware* o *software* che filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della stessa;

FLOPPY DISK: supporto di memorizzazione che contiene all'interno di un contenitore quadrato o rettangolare di plastica un disco sottile e flessibile (in inglese "floppy") su cui vengono memorizzati magneticamente i dati;

FORUM insieme delle sezioni di discussione di una piattaforma informatica;

GIOCHIDAZZARDO: sono i siti che AAMS (Amministrazione autonoma dei monopoli di Stato) segnala non in regola con il pagamento dei diritti, e che vanno bloccati per legge;

GPRS: (General Packet Radio Service): è uno standard per comunicazioni cellulari che consente trasmissioni fino a 150 Kb al secondo. Rappresenta una soluzione particolarmente adatta alla spedizione e ricezione di posta elettronica o alla navigazione *web* con terminali cellulari;

HARD DISK: tipologia di dispositivo di memoria di massa che utilizza uno o più dischi magnetici per l'archiviazione dei dati;

HARDWARE: parte fisica del computer, ovvero di tutte quelle parti magnetiche, ottiche, meccaniche ed elettroniche che lo compongono;

HOSTING: designa il servizio di gestione di un sito *web* ospitato su un elaboratore aziendale;

INPUT: insieme di elementi in entrata, per realizzare o produrre qualcosa;

INTERNET PROVIDER : l'Azienda che fornisce alla CCIAA il canale di accesso ad Internet;

INDIRIZZO IP: è un numero che identifica univocamente un dispositivo collegato a una rete informatica che comunica utilizzando lo standard IP(protocollo informatico), ossia un protocollo di rete a pacchetto, non connesso;

IRC (Internet Relay Chat): è stata la prima forma di comunicazione istantanea (*chat*) su Internet. Consente sia la comunicazione diretta fra due utenti che il dialogo contemporaneo di interi gruppi di persone in *stanze* di discussione chiamate *canali*;

LOG: registrazione cronologica delle operazioni e il *file* su cui tali registrazioni sono memorizzate;

MAILING-LIST: lista di utenti interessati allo scambio di informazioni su un argomento comune, utilizzando la posta elettronica;

NETWORKING: rete di telecomunicazioni che permette lo scambio o condivisione di dati informativi e risorse;

OUTPUT: Informazioni o segnali provenienti dal computer e diretti verso una periferica esterna ad esso; l'*output* consiste generalmente in dati stampati su carta, visualizzati sul monitor;

PEER TO PEER: si intende una rete di computer o qualsiasi rete informatica che non possiede nodi gerarchizzati come *client* o *server* fissi (clienti e serventi), ma un numero di nodi equivalenti (in inglese *peer*) che fungono sia da cliente che da servente verso altri nodi della rete;

PHISHING: siti noti per ospitare siti dolosi, quali truffe via Internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili;

PORTA : è una connessione attraverso cui vengono mandati e ricevuti dati;

POST messaggio testuale, con funzione di opinione o commento, inviato in uno spazio comune su Internet per essere pubblicato;

PROXY: programma che si interpone tra un *client* ed un *server*, inoltrando le richieste e le risposte dall'uno all'altro;

PROXY AVOIDANCE: siti di navigazione anonima che, se non bloccati, rendono inutile il filtraggio del proxy;

RESET: ripristino delle situazioni iniziali di un sistema di elaborazione;

ROAMING: il *roaming* (Rintracciabilità nel territorio) identifica nelle reti telematiche e di telecomunicazione un insieme di normative e di apparecchiature che permettono di mettere in comunicazione due o più reti distinte. Il *roaming* viene utilizzato dagli operatori telefonici di telefonia cellulare per permettere agli utenti di collegarsi utilizzando una rete non di loro proprietà. Ciò può accadere quando l'*utente* si trova all'estero e l'operatore telefonico non ha una rete propria, oppure quando l'*utente* si trova nel paese di origine dell'operatore telefonico ma questo non ha una copertura totale della nazione, (in questo caso l'operatore si appoggia sulle reti telefoniche di altri operatori). Attraverso il *roaming*, quindi, l'operatore consente all'*utente* la possibilità di utilizzare il servizio in tutta la nazione;

SCORM: "Shareable Content Object Reference Model" (Modello di Riferimento per gli Oggetti di Contenuto Condivisibili). E' tecnicamente un "modello virtuale" (*reference model*), cioè una raccolta di specifiche tecniche che consente lo scambio di contenuti digitali in maniera indipendente dalla piattaforma;

SCREEN SAVER: è un'applicazione per computer che provoca l'oscuramento dello schermo o la comparsa di un'animazione o di una serie di immagini in successione sullo stesso dopo un periodo programmato di inattività del mouse e della tastiera (non dell'elaboratore in sé), impostabile attraverso un timer;

SERVER: designa il o i computer utilizzati dalla Camera di Commercio per fornire i servizi previsti;

SISTEMA INFORMATICO: un insieme di computer, composti da *hardware* e *software* che elaborano dati e informazioni per restituire altri dati ed informazioni utili;

SISTEMA INFORMATIVO della Camera di Commercio I.A.A. di Trento: l'insieme coordinato dell'infrastruttura di rete telematica e degli apparati, computer, stampanti, *software* archiviati e/o risorse informative a qualsiasi titolo archiviate in modo digitale, in dotazione ed uso all'Ente camerale;

SOFTPHONE: in informatica un *softphone* è un programma *software* per effettuare chiamate telefoniche su internet utilizzando un computer di uso generale, piuttosto che utilizzare *hardware* dedicato. Spesso un *softphone* è stato progettato per comportarsi come un telefono tradizionale. A volte appare come l'immagine di un telefono cellulare, con un pannello del display e pulsanti con i quali l'*utente* può interagire. Un *softphone* di solito è usato con un auricolare collegato alla scheda audio del PC, o con un telefono USB;

SOFTWARE: termine generico che indica l'insieme dei programmi che permettono di far eseguire al computer specifiche istruzioni;

SPYWARE EFFECTS/PRIVAC CONCERNS: siti associati ad azioni di raccolta di dati personali non autorizzata;

SPYWARE/MALWARE SOURCES: siti contenenti malware e cioè software creati con il solo scopo di causare danni più o meno gravi ad un computer o ad un sistema informatico su cui viene eseguito;

STORAGE: con tale termine si identificano i dispositivi *hardware*, i supporti per la memorizzazione, le infrastrutture ed i *software* dedicati alla memorizzazione non volatile di grandi quantità di informazioni in formato elettronico;

TITOLARE DEL TRATTAMENTO: la persona fisica o giuridica o altro organismo cui competono le decisioni in ordine alle finalità e modalità del trattamento dei dati personali, compreso il profilo della sicurezza;

UPLOAD: processo di invio o trasmissione di un *file* (o più genericamente di un flusso finito di dati o informazioni) ad un sistema remoto attraverso una rete informatica;

UTENTE: chiunque – dipendente e non – abbia ricevuto dall'Ente camerale le credenziali per l'utilizzo del *Sistema informatico* della Camera di Commercio I.A.A. di Trento, sia che il collegamento avvenga in rete locale che in accesso remoto, e che è per questo tenuto ad osservare le prescrizioni del presente Disciplinare;

WAP: Wireless Application Protocol. Tecnologia per il collegamento di telefoni cellulari a sistemi di posta elettronica o a siti Internet appositamente realizzati (solo testo);

WEB: un insieme vastissimo di contenuti multimediali e di servizi di Internet, contenuti e servizi che possono essere resi disponibili dagli stessi utenti di Internet;

WHITE LIST: elenco di siti direttamente e immediatamente accessibili da tutti gli utenti internet;

WIKI: pagina *web* (o collezione di documenti ipertestuali) che viene aggiornata dai suoi utilizzatori e i cui contenuti sono sviluppati in collaborazione da tutti coloro che vi hanno accesso.

Allegato 1 – Esempio di Scheda per la richiesta di attivazione di credenziali di autenticazione

MODALITA' DI ACCESSO ALLA RETE ED AI SERVIZI CAMERALI		TIPO RAPPORTO E CODICE UTENTE								CARTELLE DATI					CARTELLE CONDIVISE OUTLOOK			POSTA ELETTRONICA CONDIVISA REINDIRIZZATA					ACCESSIBILITA' AREA APPLICATIVA											RISORSE USB	ACCESSO INTERNET	E-MAIL nominativa (nome.cognome@dominio)
																							Active Directory/Desktop								Intranet					
	Data agg.to	CCIAA	Accademia	TrentiniSprint	Trentino Spa	Tsm	Consulente	stagista		cartella comune C.C.I.A.A.	cartella assegnata in via esclusiva	Applicativi specifici dell'Ufficio	...	...	Ufficio	...	...	...	...	...	...	...														
UFFICIO AFFARI ISTITUZIONALI (UAI)																																				
Dipenente XY...																																				
utenza altri Uffici																																				
utenza dismessa																																				
TOTALI		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Situazione al

Visto e sottoscritto !

Il Direttore dell'Ufficio...

Da restituire all'Ufficio Sistemi Informatici

Allegato 2 - Modello di richiesta per la disattivazione delle credenziali di autenticazione

Trento, _____

Spett.le
Camera di Commercio I.A.A. di Trento
Ufficio Sistemi Informatici
Sede camerale

Oggetto: Richiesta disattivazione credenziali di accesso al sistema informativo camerale ***(da riconsegnare debitamente compilata al Direttore dell'Ufficio per l'inoltro all'Ufficio Sistemi Informatici unitamente alla scheda informatica aggiornata dell'Ufficio)***

Il sottoscritto _____ , terminato il tirocinio/l'incarico/il rapporto di lavoro presso l'Ufficio _____

COMUNICA

- di aver provveduto alla cancellazione di tutti i dati personali eventualmente contenuti all'interno della casella nominativa di posta elettronica e delle Directory assegnategli in via esclusiva;
- di aver impostato in Outlook la "regola del fuori sede" comunicando la cessazione del *tirocinio/incarico/rapporto di lavoro* e l'indirizzo sostitutivo _____@tn.camcom.it, segnalato dal Direttore d'Ufficio, per l'inoltro di e-mail all'Ufficio;

Distinti saluti.

Firma _____

* * *

Il Direttore dell'Ufficio _____

RICHIEDE

1. la disattivazione delle credenziali di accesso al sistema informativo camerale a partire dal_____;
2. la disattivazione della casella di posta elettronica a partire dal_____.

Firma _____

Allegato 3 – Procedure per l'attivazione dell'assistenza informatica remota

Premessa

L'Amministrazione camerale è in possesso dei seguenti software che permettono l'assistenza remota:

1. Praim Thinman Remote Console;

2. Citrix Shadow Taskbar;

3. Citrix Desktop Director.

Detti software non sono "normalmente" attivi e vengono attivati per specifiche esigenze di supporto tecnico generalmente richiesto dagli utenti.

L'utilizzo dei software è dettato infatti dalla principale necessità di adempiere in maniera efficiente e puntuale alle richieste provenienti quotidianamente dai dipendenti camerali che usano le postazioni informatiche messe a loro disposizione dall'Amministrazione, consentendo un notevole risparmio di tempo e di risorse economiche ed umane, nonché la possibilità di eseguire un maggior numero di interventi giornalieri in favore degli assistiti.

Tali software consentono inoltre agli Amministratori di sistema di svolgere altre funzioni di tipo diagnostico e manutentivo sul sistema informatico camerale.

Il personale camerale in capo all'Ufficio Sistemi Informatici, autorizzato in qualità di Amministratore di sistema all'utilizzo di detti software per operazioni di assistenza informatica remota, effettuerà esclusivamente le operazioni necessarie al supporto, all'assistenza ed al ripristino di funzionalità operative ed applicative richieste dall'utente, rispettando rigorosamente la riservatezza dei dati di cui accidentalmente venisse a conoscenza nel corso dell'attività che è tenuto a svolgere.

I software per l'assistenza remota sono utilizzati nel rispetto della normativa vigente in particolare con riferimento all'obbligo di non adibire tali strumenti a finalità di controllo dei lavoratori ed alla salvaguardia della privacy (D.Lgs. 30 giugno 2003, n. 196).

Si riportano di seguito i dettagli tecnici delle tre procedure di assistenza informatica remota disponibili.

In caso di cambiamento radicale l'eventuale cambio di versione (release) o migrazione ad altra applicazione sostitutiva sarà preventivamente portata a conoscenza delle organizzazioni.

****

Schede tecniche

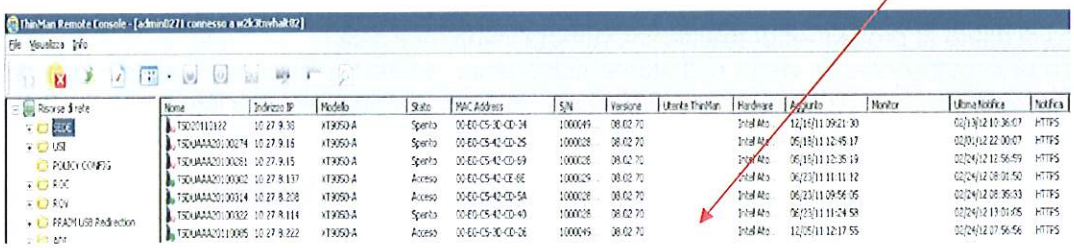
L'assistenza informatica remota viene attivata normalmente in seguito ad una richiesta di supporto da parte dell'utente o per necessità tecniche di manutenzione riscontrate da parte dell'Ufficio Sistemi Informatici. Può pervenire mediante contatto telefonico con l'Ufficio Sistemi Informatici o può comunque essere concordata, anche in modalità telematica, in seguito ad una richiesta di supporto inoltrata tramite il sistema telematico di helpdesk denominato "Assistel" o in seguito ad una valutazione tecnica di manutenzione da parte dell'Ufficio Sistemi Informatici.
L'utente deve essere fisicamente davanti alla postazione per poter acconsentire all'avvio della procedura di assistenza. L'opportunità della richiesta di assistenza remota da parte dell'utente viene valutata dal Referente Informatico della Unità organizzativa a cui appartiene, il quale sarà tenuto inoltre a sovraintendere alle procedure di supporto tecnico eseguite nel contesto dell'assistenza remota.
La scelta del software da utilizzare per l'assistenza informatica remota viene fatta dall'Amministratore di sistema in capo all'Ufficio sistemi informatici in base alle condizioni tecniche ed operative contingenti.

1. *Thinman Remote Console*

Questa modalità viene utilizzata per collegarsi direttamente sulla postazione fisica denominata "Thinclient Praim" al fine di poter assistere l'utente per i tutti i "desktop virtualizzati" (sia di tipo Xenap che Xendesktop) a cui lo stesso utente può essere abilitato.
Tale modalità viene preferita alle altre per i seguenti motivi:

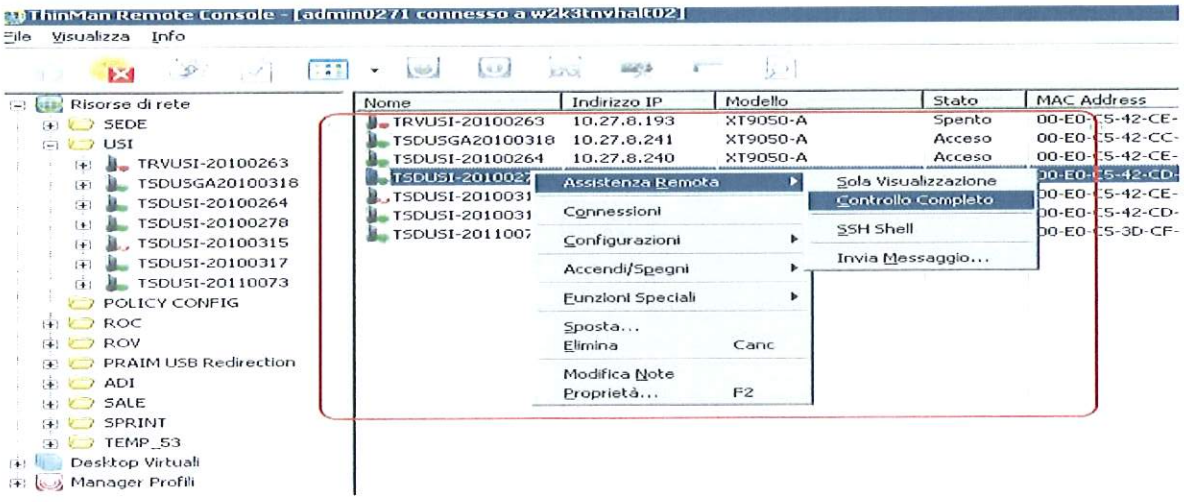
1. è' integrata in una piattaforma di amministrazione e di gestione completa delle postazioni;
2. permette un utilizzo ed una operatività più performante e risponde meglio ai comandi di interazione con l'utente;
3. riesce a offrire un sistema di pieno supporto, sia della postazione fisica che delle postazioni "virtualizzate" che lo stesso utente sta utilizzando.

L'Amministratore di sistema utilizza la seguente interfaccia principale con **l'elenco dei dispositivi "Thinclient Praim"** installati nella rete e corrispondenti alle postazioni fisiche degli utenti..



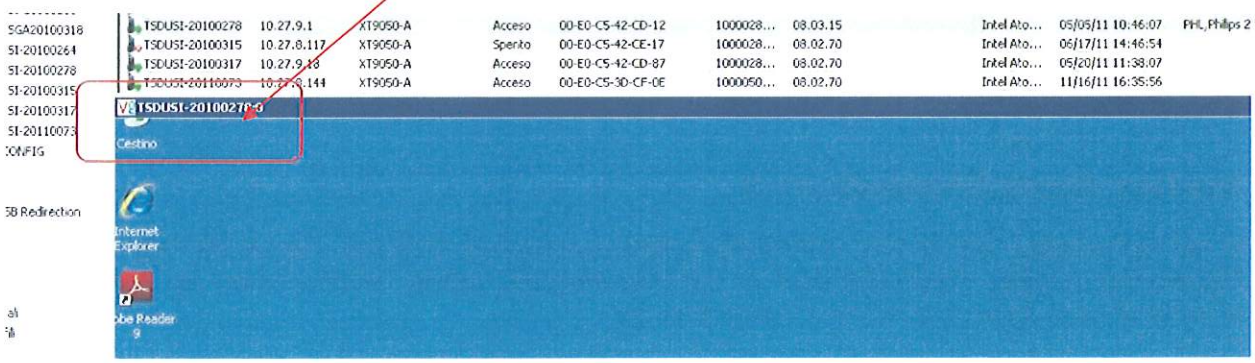
Modalità di richiesta di assistenza remota

In corrispondenza del codice identificativo della postazione utilizzata dall'utente che ha richiesto l'assistenza remota, l'Amministratore di sistema procede, previa identificazione per via telefonica, all'avvio della procedura di richiesta di connessione.

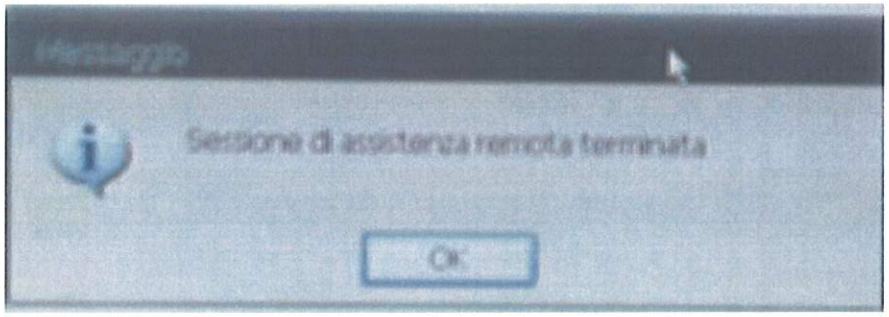


Un messaggio in **popup** compare sulla postazione dell'utente per richiedere l'accettazione della richiesta di assistenza. L'utente può accettare o rifiutare.

In caso di rifiuto la procedura di assistenza remota viene interrotta.
In caso di accettazione da parte dell'utente richiedente, all'Amministratore di sistema compare la **visualizzazione del desktop remoto dell'utente** e da quel momento può interagire con il desktop e quindi condividere con l'utente i contenuti del video e le azioni del mouse e della tastiera.



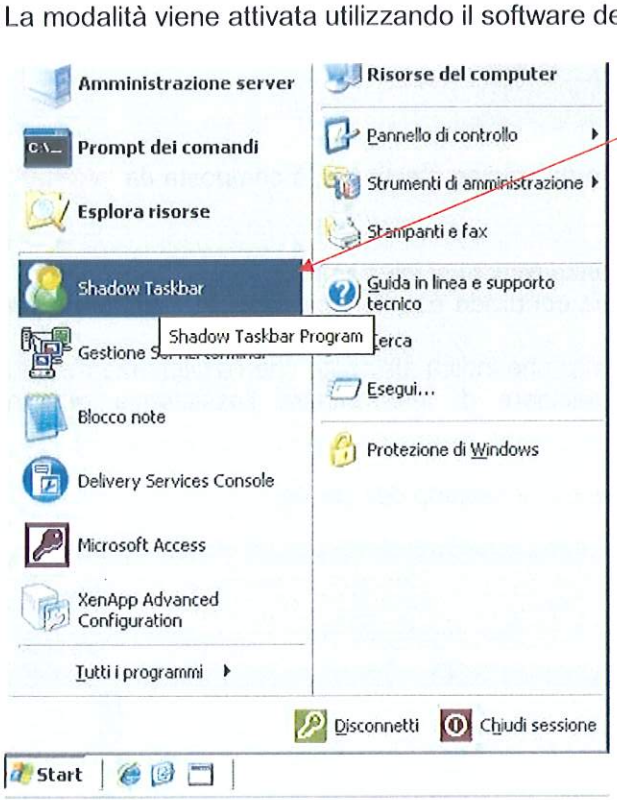
Concluso l'intervento, l'Amministratore di sistema comunicherà la chiusura dello stesso e quindi del controllo remoto e potrà inviare il seguente messaggio:



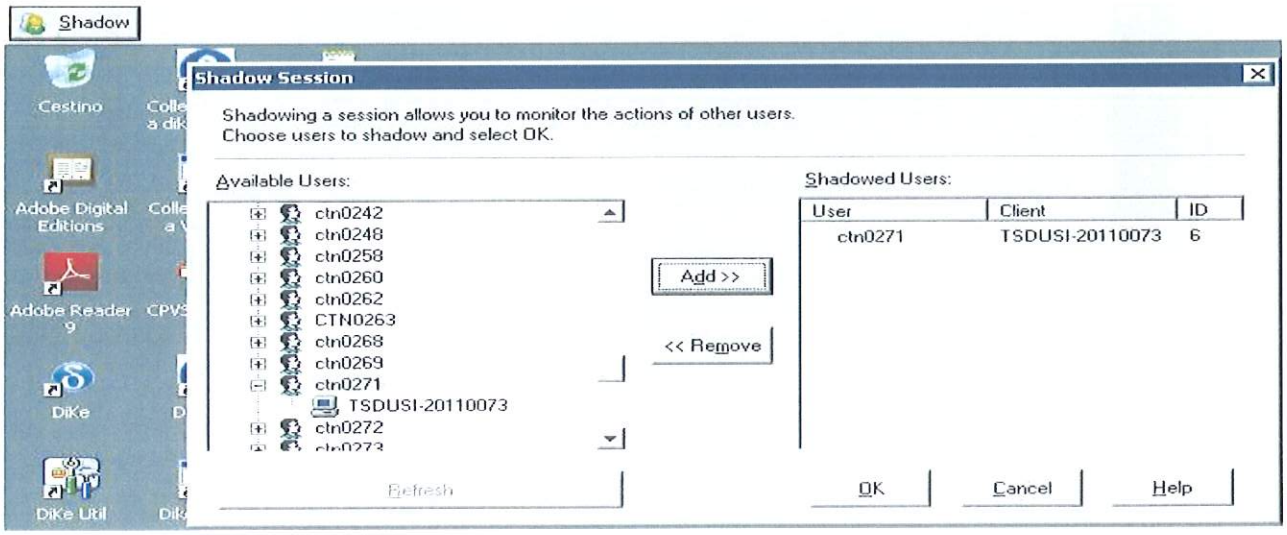
2. *Citrix Shadow Taskbar*

Questa modalità può essere utilizzata dall'Amministratore di sistema per attivare una connessione di assistenza remota direttamente e solo sulla postazione virtuale di tipo "Xenapp", indipendentemente dalla tipologia di postazione fisica in dotazione all'utente.

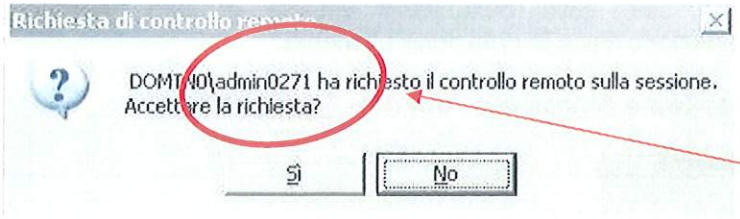
La modalità viene attivata utilizzando il software denominato **"Shadow Taskbar"**



All'Amministratore di sistema compare la **lista delle credenziali degli utenti** collegati al desktop virtuale denominato "Citrix Xenapp", abbinata al nome della postazione fisica su cui opera l'utente stesso. Dopo aver scelto la credenziale dell'utente da assistere, l'Amministratore di sistema preme sul pulsante OK per attivare la richiesta di assistenza remota.



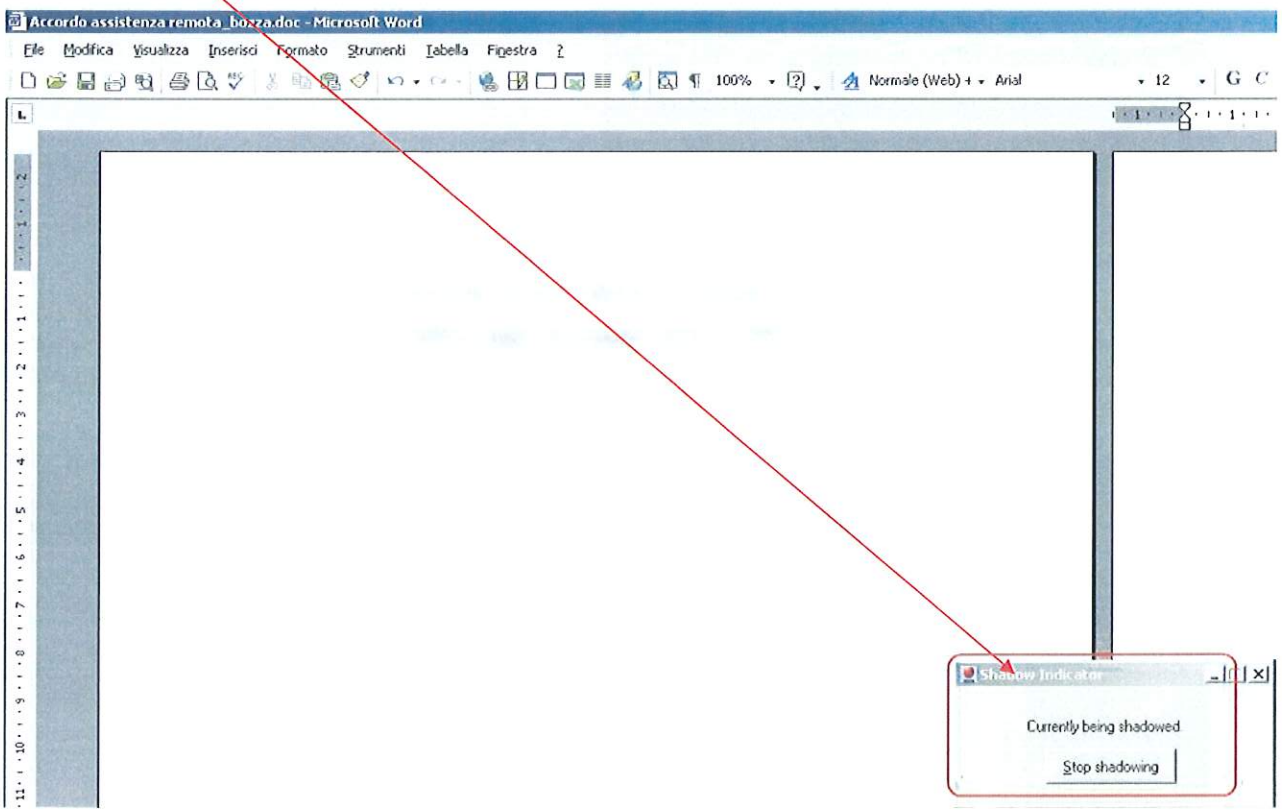
All'utente compare il seguente messaggio in popup e può accettare o rifiutare la richiesta di assistenza remota



L'Amministratore di sistema può essere identificato dal codice utente che è composta da **"admin"** e **matricola**.

In caso di non accettazione la procedura di assistenza remota si interrompe.
In caso di accettazione l'Amministratore di sistema condivide con l'utente assistito i contenuti del video e le funzioni del mouse e tastiera.
Sul desktop dell'utente compare la seguente finestra che indica all'utente che l'assistenza remota è in corso. In ogni momento l'utente può decidere di interrompere l'assistenza remota selezionando **"Stop Shadowing"**

Esempio di desktop condiviso dopo la connessione con il desktop dell'utente:

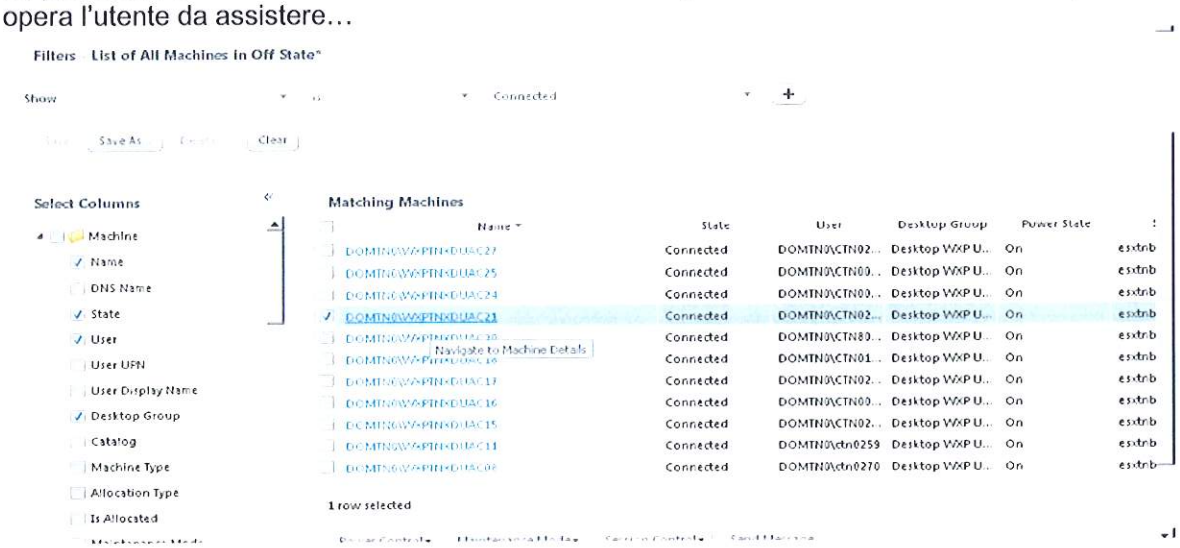


3. *Citrix Desktop Director*

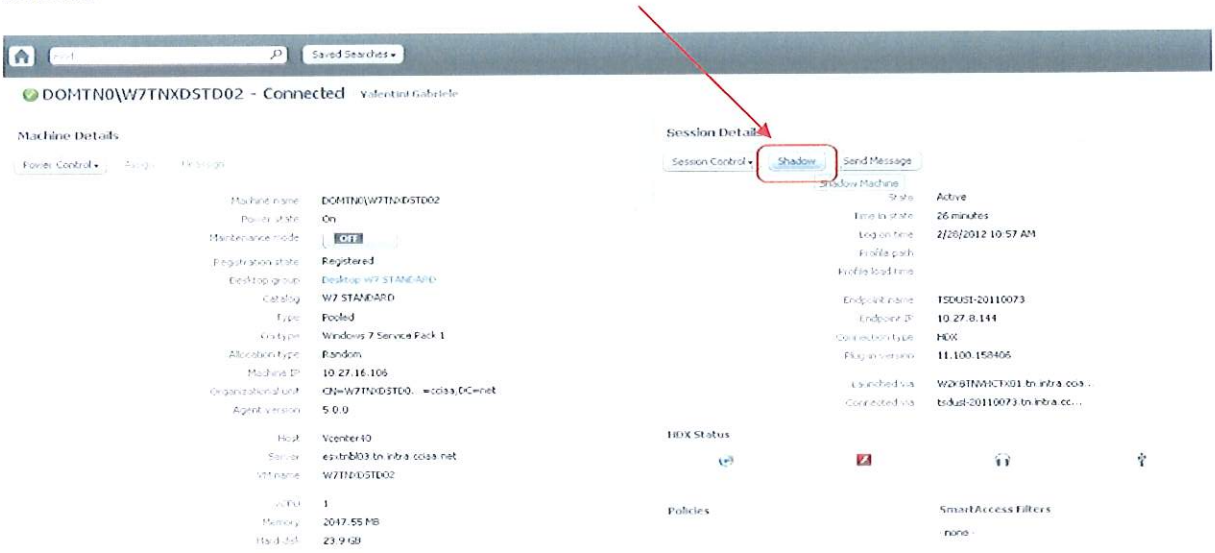
Questa modalità può essere utilizzata dall'Amministratore di sistema per attivare una connessione di assistenza remota direttamente e solo sulla postazione virtuale di tipo "Xendesktop", indipendentemente dalla tipologia di postazione fisica in dotazione all'utente.

L'accesso da parte dell'utente Amministratore di sistema avviene richiamando l'apposita applicazione software.

La procedura di inoltro di richiesta di assistenza remota prevede di selezionare il desktop su cui opera l'utente da assistere…

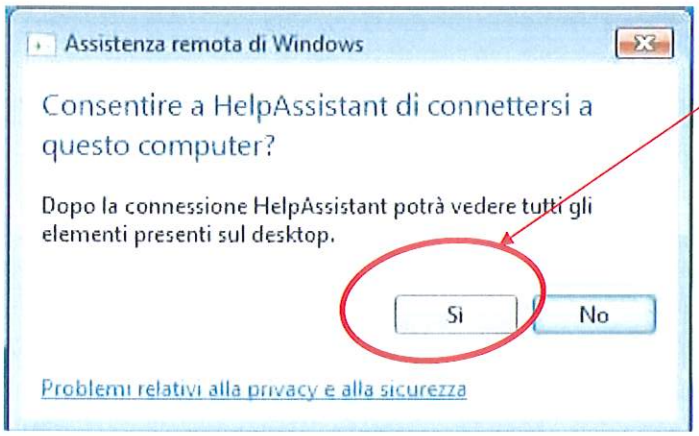


… e successivamente di premere sul pulsante "**Shadow**" per attivare la richieste di assistenza remota.

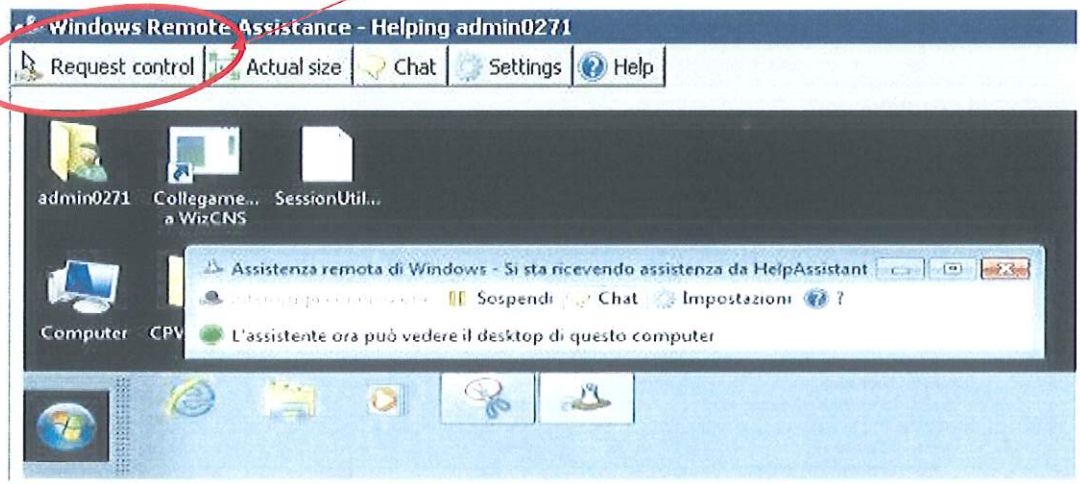


In attesa di accettazione da parte dell'utente, all'Amministratore di Sistema compare la seguente schermata:

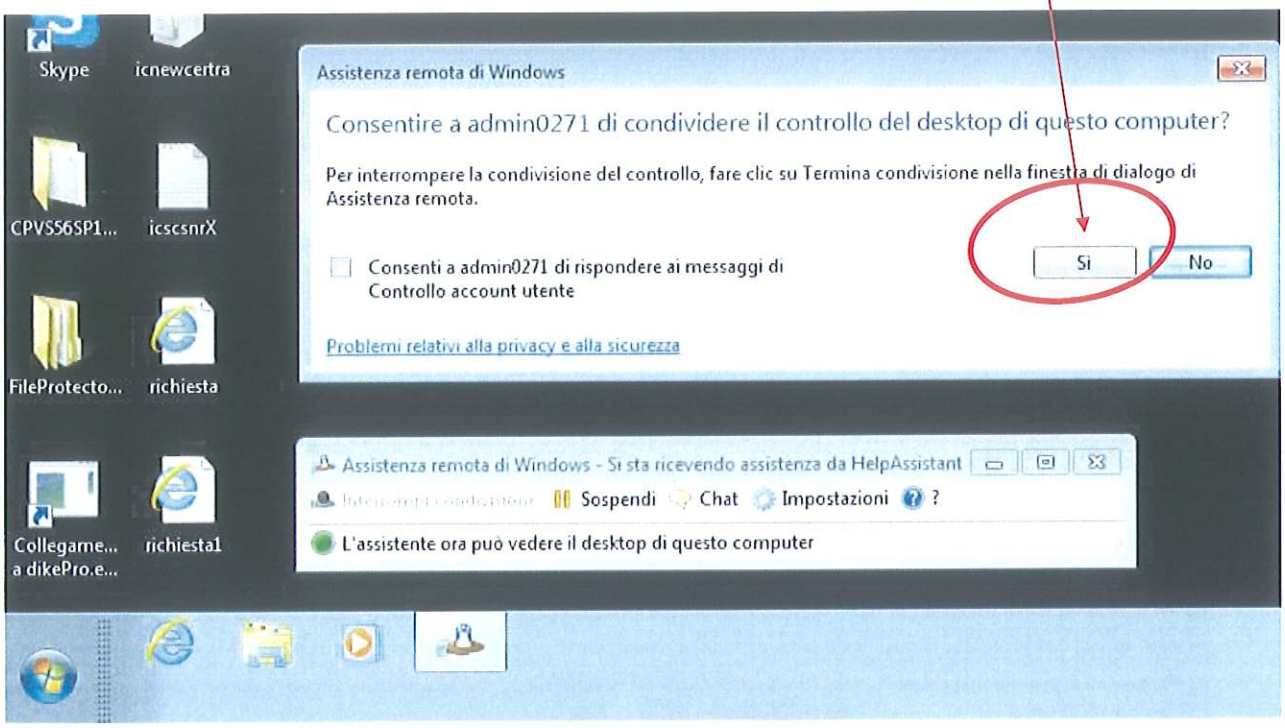
All'utente compare a video il seguente messaggio al quale deve rispondere **"Si"** per acconsentire all'attivazione dell'assistenza remota



Dopo l'accettazione della richiesta di assistenza remota, l'Amministratore di sistema può solo visualizzare il desktop dell'utente remoto. Per ottenere il pieno controllo remoto anche del mouse e della tastiera, e quindi poter gestire la sessione utente, l'Amministratore di sistema deve fare la richiesta selezionando la funzione **"Request Control"**

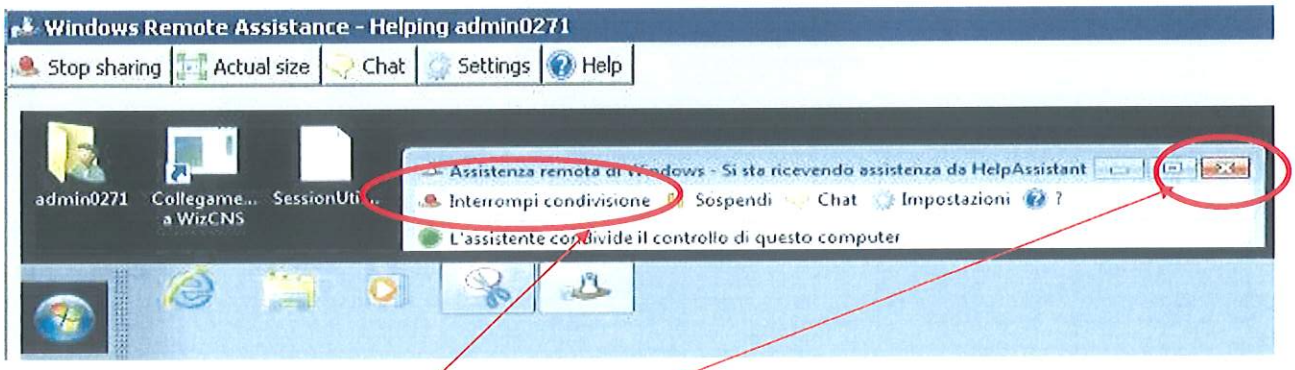


Il seguente messaggio verrà visualizzato all'utente, che deve selezionare **"Si"** per permettere all'Amministratore di sistema di gestire in modo completo la propria postazione.



L'Amministratore di sistema può essere identificato dal codice utente che è composta da **"admin"** e **matricola**.

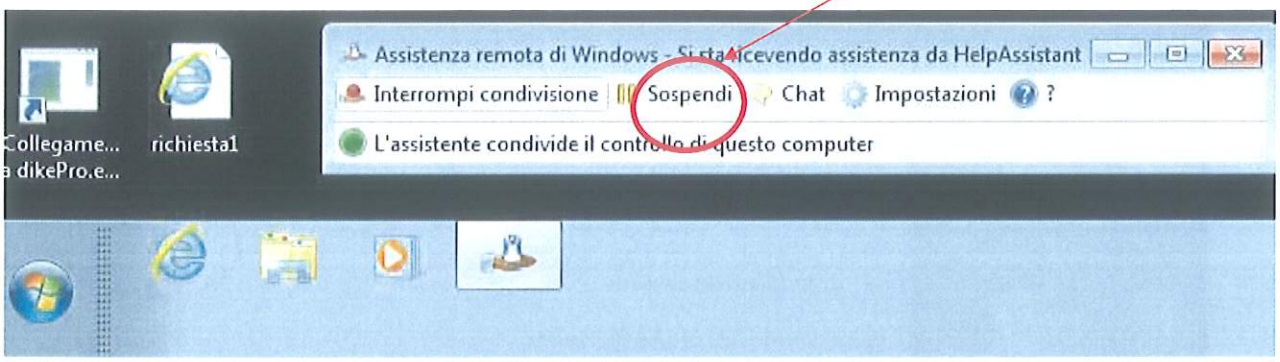
Una volta accettata la richiesta di controllo remoto l'Amministratore di sistema è in grado di operare sulla postazione dell'utente.



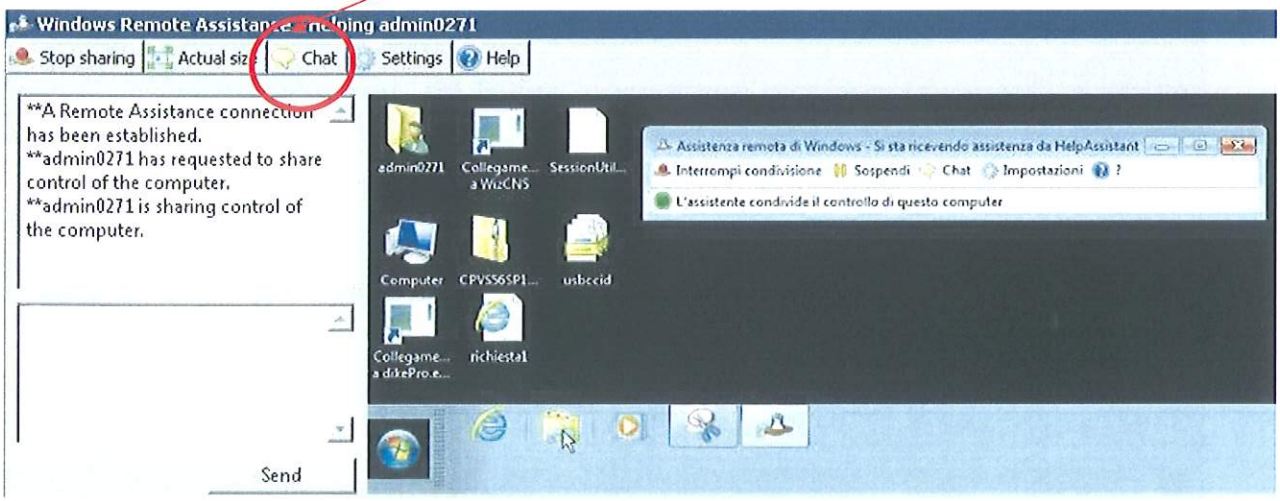
Per terminare l'operatività con mouse e tastiera nell'assistenza remota della propria sessione, l'utente può selezionare **"Interrompi condivisione"**. In questo modo l'Amministratore è ancora in grado di visualizzare il desktop utente ma non di interagire attivamente.

Per terminare l'assistenza remota l'utente può chiudere la finestra "Assistenza remota di Windows" con **X rossa** in alto a destra.

Per sospendere temporaneamente l'assistenza remota selezionare **"Sospendi"**. In questo modo l'Amministratore di sistema non è più in grado di vedere e controllare il desktop dell'utente.



Con questa modalità è inoltre possibile attivare una sessione di chat con l'Amministratore di sistema. Per attivarla si deve selezionare il pulsante **"Chat"**.
L'Amministratore di sistema visualizza sul lato sinistro la chat con l'utente



Allegato 4 – Modulo per l'assegnazione di attrezzature, strumentazioni e servizi di natura informatica per lavoro mobile

CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA - TRENTO

All'Ufficio *Sistemi Informatici/*
All'Ufficio Economato
Sede

Oggetto: Richiesta assegnazione attrezzature, strumentazioni e servizi di natura informatica per lavoro mobile.

Il sottoscritto _____, in qualità di _____ (dipendente, collaboratore, etc..) dell'Ente camerale, nel prosieguo indicato come "*assegnatario*",

d i c h i a r a

1. di ricevere, per l'espletamento delle funzioni di competenza, le seguenti attrezzature e strumentazioni informatiche:

Hardware

Descrizione	Cespite	Serial Number	Abilitazioni	Note
es. Pc Notebook HP...	*2006xxxx*			
es. Pc MCIA TimDataKit	.....	...		

Software su licenza

Descrizione	Riferimenti licenza d'uso	Note (es: Oem)
es. Microsoft Windows Xp		
es. Microsoft Office Xp Professional		
es. Symantec Antivirus client		

Tipologia di diritti di amministrazione sulla postazione

Descrizione	Contrassegnare con 'X'	Note aggiuntive
Diritti amministrativi completi		
Diritti amministrativi parziali		
Diritti power user		
Diritti user		

⌘⌘⌘

Telefonia mobile – Servizi

Descrizione	Gestore traffico	Serial Number	Abilitazioni e servizi	Numero telefonico associato
es. Sim	*Contratto Consip Telefonia mobile 4 – Tim Telecom*	*xxxxxxxxx*	*Full – dual billing – twin set*	*XXXXXXXX*

Telefonia mobile – Apparecchio

Descrizione Apparecchio	Serial Number	Noleggio/proprietà	Numero telefonico associato	Abilitazioni e servizi
es. Rim Blackberry	*XXXXXXXX*	*noleggio*	*xxxxxxxxxxx*	*Navigazione internet nazionale/posta elettronica in rete*

2. di attenersi, per la corretta gestione dei beni suindicati, alla disciplina contenuta nel vigente Disciplinare per l'utilizzo delle attrezzature informatiche e telefoniche, della posta elettronica e della rete internet, adottato dall'Ente camerale.

Trento, _____

L'Assegnatario
(Nome e Cognome)

_____

Allegato 5 – Outlook 2010: regole del "fuori sede"

In caso di assenza preventivata (ad es., per ferie o attività di lavoro fuori sede) il possessore di un *account* di Outlook dovrà impostare il proprio sistema di posta in modo che invii automaticamente messaggi di risposta contenenti le "coordinate" elettroniche e telefoniche di un altro soggetto secondo le indicazioni fornite dal Direttore dell'ufficio di appartenenza. Di seguito, si riporta un esempio della procedura per l'impostazione della Regola del "fuori sede".

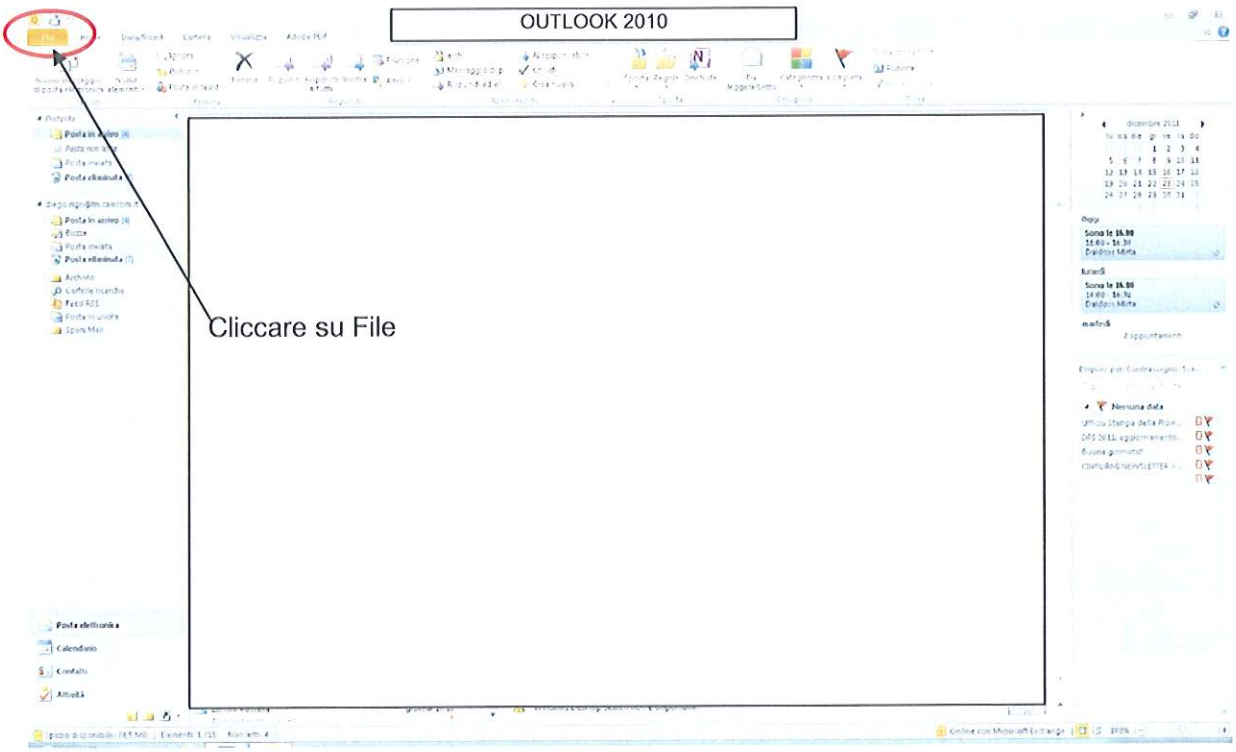


Figura 1

Figura 2

Cliccare su Risposte automatiche

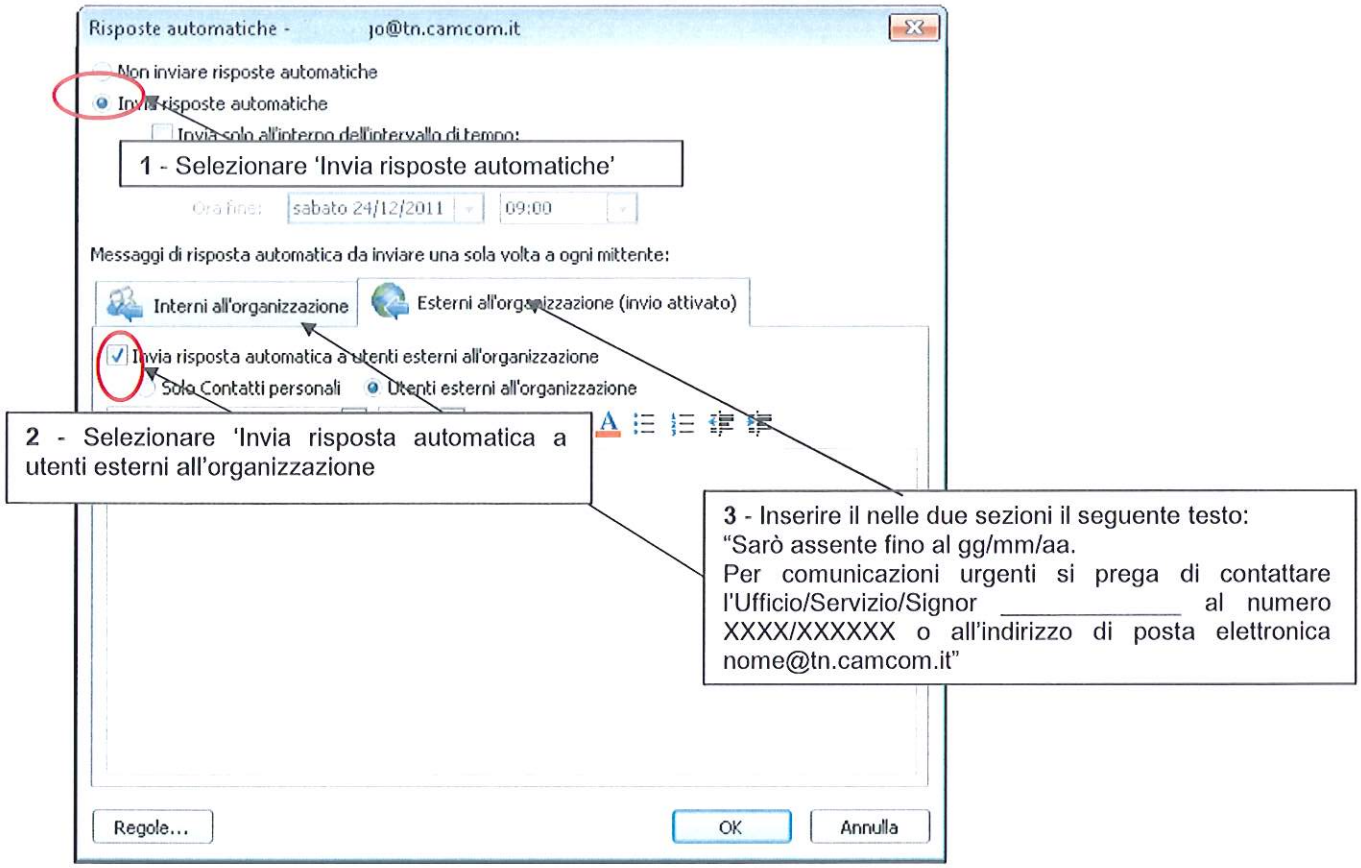

Risposte automatiche - jo@tn.camcom.it
Non inviare risposte automatiche
Invia risposte automatiche
Invia solo all'interno dell'intervallo di tempo:
1 - Selezionare 'Invia risposte automatiche'
Ora fine: sabato 24/12/2011 09:00
Messaggi di risposta automatica da inviare una sola volta a ogni mittente:
Interni all'organizzazione
Esterni all'organizzazione (invio attivato)
Invia risposta automatica a utenti esterni all'organizzazione
Solo Contatti personali
Utenti esterni all'organizzazione
2 - Selezionare 'Invia risposta automatica a utenti esterni all'organizzazione
3 - Inserire il nelle due sezioni il seguente testo:
"Sarò assente fino al gg/mm/aa.
Per comunicazioni urgenti si prega di contattare l'Ufficio/Servizio/Signor _____ al numero XXXX/XXXXXX o all'indirizzo di posta elettronica nome@tn.camcom.it"
Regole...
OK
Annulla

Figura 3

Allegato n. 6 - Dati relativi al traffico telematico oggetto di trattamento.

Il D.Lgs. 163/2003 (Codice in materia di protezione dei dati personali) prevede che i dati personali oggetto di trattamento siano custoditi e controllati in relazione alle conoscenze acquisite in base al progresso tecnico. Per tale ragione, le informazioni di carattere tecnico che seguono non possono avere carattere definitivo e devono essere considerate passibili di modifica in ragione del progresso tecnico e degli aggiornamenti normativi.

A. Dati relativi al traffico della posta elettronica

Le informazioni relative al traffico di posta elettronica e internet sono conservate:

- da InfoCamere:
  - Per ogni messaggio di posta elettronica inviato vengono registrate, sui file di log dei sistemi di posta, le seguenti informazioni:
    i. indirizzo e-mail del mittente
    ii. indirizzo e-mail del destinatario
    iii. data e ora di trattazione del messaggio
    iv. eventuali errori rilevati
    v. indirizzo ip del sistema mittente e del sistema destinatario delle mail
    vi. eventuale user-id che si è autenticato al sistema
  - Per ogni sessione di accesso alla casella di posta elettronica vengono registrate, sui file di log dei sistemi, le seguenti informazioni:
    i. user-id che si collega
    ii. data e ora dell'apertura (log-in) e della chiusura (log-out) della sessione
    iii. eventuali errori di colloquio
  - Il periodo di conservazione delle informazioni relative al traffico di posta elettronica è pari a 12 mesi.
- Dall'Ente camerale:
  - Per ogni messaggio di posta elettronica inviato vengono registrate, sui file di log dei sistemi di posta, le seguenti informazioni:
    i. indirizzo e-mail del mittente
    ii. indirizzo e-mail del destinatario
    iii. data e ora di trattazione del messaggio
  - Il periodo di conservazione delle informazioni relative al traffico di posta elettronica è pari a 28 giorni.

B. Dati relativi al traffico internet:

Le informazioni relative al traffico internet sono conservate da InfoCamere.

- per ogni accesso ad Internet vengono registrate, sui file di log dei sistemi, le seguenti informazioni:
  i. indirizzo IP del client
  ii. user-id dell'utente
  iii. data e ora dell'accesso al sito visitato
  iv. indirizzo (URL) della risorsa Internet acceduta
  v. return code http
  vi. numero di byte scaricati
- Il periodo di conservazione delle informazioni relative al traffico telematico è pari a 12 mesi.

C. Filtri che bloccano l'accesso ai siti internet:

- I filtri standard che bloccano l'accesso ai siti sono applicati da InfoCamere e appartengono alle seguenti categorie:
  - *Giochidazzardo*
  - *phishing*
  - *proxy avoidance*
  - *spyware effects/privacy concerns*
  - *spyware/malware sources*
  - pornograpy

Allegato 7 – Verbale di Ispezione delle Postazioni di Lavoro

CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA - TRENTO

Verbale di ispezione di postazione di lavoro

(ai sensi del punto 18.3 del Disciplinare per l'utilizzo delle attrezzature informatiche e telefoniche, della posta elettronica e della rete internet)

Io sottoscritto _____, in qualità di Segretario Generale / delegato del Segretario Generale incaricato formalmente dal Segretario Generale con nota di data _____, per la seguente motivazione _____,

ho provveduto in data _____, con l'ausilio tecnico dell'*Amministratore di sistema* _____[, indicatomi dal Segretario Generale,] a effettuare l'ispezione della postazione di lavoro del dipendente _____, identificata dal codice _____.

L'ispezione è avvenuta in presenza di _____ e del dipendente/suo delegato_____.

Le operazioni di ispezione sono state le seguenti:

_____

Provvedo a consegnare copia del presente verbale al dipendente ed ai seguenti soggetti interessati _____.

Trento, _____

Il Segretario Generale/
Il delegato del Segretario Generale

_____

Per presa visione:
Il Direttore d'Ufficio

_____

Il Dipendente

_____

Allegato 8 – Verbale di accesso alla mailbox/postazione informatica del lavoratore assente

CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA - TRENTO

Verbale di accesso alla mailbox/postazione informatica assegnata al lavoratore assente

(ai sensi del punto 20.1 lett. g) del Disciplinare per l'utilizzo delle attrezzature informatiche e telefoniche, della posta elettronica e della rete internet)

Io sottoscritto _____, in qualità di Direttore dell'Ufficio_____, incaricato formalmente dal Dirigente dell'Area___ - _____ con nota di data _____, a seguito della assenza *improvvisa/prolungata* del dipendente camerale _____ risultato *irragiungibile/ impossibilitato ad avvalersi del sistema di web-mail*, per improrogabili necessità legate all'attività lavorativa *(specificare la motivazione)*_____, ho provveduto in data _____, con l'ausilio tecnico dell'*Amministratore di sistema* _____, indicatomi dal Dirigente _____, a verificare il contenuto dei messaggi/file ritenuti rilevanti per lo svolgimento dell'attività lavorativa presenti nella mailbox nome.cognome@tn.camcom.it/*nella directory* denominata _____ e assegnata in via esclusiva *al dipendente* _____ .

I messaggi/file *visionati/prelevati* sono stati i seguenti:

_____

_____

Provvedo a consegnare copia del presente verbale al Dirigente dell'Area ___ - _____, al Direttore dell'Ufficio Risorse Umane e al dipendente al suo rientro in servizio.

Trento, _____

Il Direttore dell'Ufficio _____

_____

Per presa visione:

Il Dirigente dell'Area ___ - _____

_____

Il Direttore dell'Ufficio Risorse Umane

_____

Il Dipendente

_____

Riservato all'Amministratore di sistema

Dichiaro di aver proceduto su incarico del Dirigente _____a resettare la password collegata alla user-id _____, afferente il sig. _____, e di aver collegato alla stessa *user-id* la nuova password _____ che ho comunicato a _____ _____ alle ore _____ del giorno_____.
Ho successivamente provveduto a bloccare la nuova password alle ore _____ del giorno _____.

Nome e Cognome dell'AdS
FIRMA

_____

Allegato 9 – Disclaimer

1. DISCLAIMER PER MESSAGGI DI POSTA ELETTRONICA

Ai sensi del Codice in materia di protezione dei dati personali (D.Lgs. 196/03) il contenuto di questa e-mail e degli eventuali allegati è riservato e ad uso esclusivo del destinatario. Chiunque riceva questa e-mail per errore è pregato di distruggerla e contattare telefonicamente la Camera di Commercio I.A.A. di Trento al numero 0461/887 ___.
Si informa inoltre che la risposta alla presente e-mail compresi eventuali allegati potrebbero essere visionati, ai fini del disbrigo delle attività d'ufficio, anche da altro personale incaricato.

This e-mail may contain confidential and/or privileged information. If you are not the addressee (or have received this e-mail in error) please notify the sender immediately (tel. nr: 039 0461 887 ___) and destroy this e-mail. Any unauthorised copying, disclousure or distribution of the material in this e-mail is strictly forbidden and could be a crime. Ref. D. Lgs. 196/2003.

Please also note that the e-mail messages, as well as their attachments, may be read, for office's tasks, by other members of our staff.

2. DISCLAIMER PER COPERTINA FAX

Ai sensi del Codice in materia di protezione dei dati personali (D.Lgs. 196/03), il contenuto di questo fax e degli eventuali allegati è riservato e ad uso esclusivo del destinatario. Qualora questo messaggio fosse da Voi ricevuto per errore, vogliate cortesemente darcene notizia a mezzo telefax e distruggere il messaggio.

If you have received this telefax message in error please notify the sender immediately and destroy this document. Any unauthorised copying, disclousure or distribution of the material in this document is strictly forbidden and could be a crime. Ref. D. Lgs. 196/2003.

Allegato 10 – Procedura di partecipazione alle iniziative in modalità FAD

- L'iscrizione seguirà le stesse modalità finora previste per la formazione tradizionale; al momento dell'attivazione dell'iniziativa formativa verrà comunicato al dipendente se si svolgerà in modalità tradizionale o in FAD.
- Il dipendente, prima di accedere alla lezione on line, dovrà inserire l'idoneo giustificativo nell'apposito applicativo per la gestione delle presenze o su modulo cartaceo. Il suddetto giustificativo, rispetto esclusivamente alla formazione on line, sostituirà la timbratura.
- Considerato che durante la formazione on line viene sospesa l'attività di servizio, è necessario adottare alcuni accorgimenti atti, da una parte, a garantire il diritto del partecipante alla formazione e, dall'altra, a ridurre i possibili disservizi derivanti dall'interruzione dell'attività. Ad esempio, si raccomanda di concordare con il Direttore d'Ufficio le modalità di fruizione e, in particolare, di scegliere un orario non di apertura al pubblico, deviare le chiamate telefoniche, avvisare i colleghi affinché provvedano a sostituire il partecipante durante il tempo di formazione.
- Per facilitare il dipendente nello svolgimento della lezione on line e per non pregiudicare l'attività di servizio, si raccomanda di informare dirigente e/o direttore dell'avvio della formazione a distanza.
- Il dipendente è tenuto a partecipare all'edizione a cui risulta iscritto; sarà consentita la possibilità di recupero esclusivamente qualora l'articolazione del corso lo consenta.
- Per ogni iniziativa formativa sarà prevista una scadenza entro la quale il dipendente dovrà completare il corso di formazione e compilare il test conclusivo di apprendimento, quando previsto.
- Il corso potrebbe risultare non svolto qualora non siano rispettate le disposizioni previste nel presente allegato e le indicazioni comunicate di volta in volta riguardanti le specifiche iniziative.