CAMERA DI COMMERCIO, INDUSTRIA, ARTIGIANATO E AGRICOLTURA DI PAVIA

DISCIPLINARE PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI, DELLA RETE INFORMATICA E TELEMATICA (INTERNET E POSTA ELETTRONICA) E DEL SISTEMA DI TELEFONIA FISSA E MOBILE

INDICE

PREMESSA

Sezione I – DISPOSIZIONI GENERALE

Art. 1 – FINALITA'

Art. 2 – PRINCIPI GENERALI

Art. 3 - DESTINATARI

Sezione II – USO DEGLI STRUMENTI INFORMATICI, TELEMATICI E DI TELEFONIA

Art. 4 – CRITERI GENERALI DI UTILIZZO

Art. 5 – UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 6 – UTILIZZO DELLA RETE INFORMATICA INTERNA

Art. 7 – REGOLE COMPORTAMENTALI

Art. 8 – UTILIZZO DELLA RETE INTERNET

Art. 9 – UTILIZZO DELLA POSTA ELETTRONICA

Art. 10 – GESTIONE DELLE CREDENZIALI DI ACCESSO

Art. 11 – UTILIZZO DEGLI STRUMENTI DI TELEFONIA FISSA E MOBILE

Sezione III – CONTROLLO E SANZIONI

Art. 12 – MODALITA' DI EFFETTUAZIONE DEI CONTROLLI

Art. 13 - SANZIONI

Sezione IV – DISPOSIZIONI FINALI

Art. 14 – DISPOSIZIONI FINALI

PREMESSA

La Camera di Commercio, Industria, Artigianato e Agricoltura di Pavia promuove ed incentiva l'utilizzo sempre più diffuso della rete informatica e telematica, con particolare riferimento all'uso di internet, della posta elettronica e del sistema di telefonia fissa e mobile quali moderne tecnologie che, nell'ambito dello svolgimento dell'attività lavorativa dei propri dipendenti, consentono di perseguire con maggior efficacia, efficienza ed economicità le finalità istituzionali dell'Ente in un'ottica di semplificazione dell'attività amministrativa.

Inoltre, attraverso l'adozione del presente Disciplinare - volto, da un lato, a sensibilizzare il personale camerale, il personale dell'Azienda Speciale Paviasviluppo, i collaboratori, nonché gli organi, a un uso delle tecnologie dell'informazione e della comunicazione coerente con l'attività lavorativa, e dall'altro, ad assicurare il giusto contemperamento tra le esigenze organizzative della Camera, quale datore di lavoro, e quelle di tutela della riservatezza dei dati personali dei lavoratori nel rispetto della vigente normativa in materia di privacy, di cui al Regolamento UE 679/2016, al Codice in materia di protezione dei dati personali (D. Lgs. del 30 giugno 2003, n. 196 – Codice Privacy - come modificato dal D. Lgs. 101/2018) e ai Provvedimenti del Garante per la protezione dei dati personali (Garante Privacy) - la Camera (d'ora in poi intesa anche come Azienda Speciale Paviasviluppo) intende assicurare la funzionalità e il corretto impiego della strumentazione informatica a disposizione del proprio personale.

La Camera di Pavia, al fine di incrementare il livello di sicurezza e semplificare la gestione degli strumenti informatici, ha adottato la tecnologia Virtual Desktop Infrastructure (VDI) che consente di avere postazioni di lavoro sempre performanti e configurate in modo idoneo alle sole attività lavorative. Al desktop virtuale si accede, con user-id e password, attraverso il pc fisico.

Sezione I

DISPOSIZIONI GENERALI

Art. 1
FINALITA'

1. Il presente Disciplinare è finalizzato a garantire efficienza, efficacia ed economicità dell'attività amministrativa, nel rispetto della normativa vigente in materia di tutela della privacy, attraverso la disciplina dell'uso delle risorse tecnologiche e informatiche e la responsabilizzazione dei lavoratori/utilizzatori in merito all'eventuale uso delle stesse in modo non coerente con l'attività lavorativa, con gli interessi dell'Ente e con le norme che disciplinano il lavoro nelle pubbliche amministrazioni.
2. In particolare è diretto a:
   a) porre in essere ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri degli strumenti informatici, della Rete Informatica e Telematica e del Sistema di telefonia fissa e mobile, nel rispetto dei diritti dei lavoratori e del diritto alla riservatezza;
   b) informare coloro che utilizzano per lavoro gli strumenti informatici, la Rete Informatica e Telematica e il Sistema di telefonia messi a disposizione dalla Camera,

delle misure adottate e che si intendono adottare al fine di:

- garantire il diritto alla riservatezza degli utenti interni ed esterni della Rete Informatica, Telematica e del Sistema di Telefonia;
- assicurare la funzionalità ed il corretto impiego delle strumentazioni informatiche e telematiche da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa;
- prevenire rischi alla sicurezza del sistema;
- responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle strumentazioni, rendendoli consapevoli che ogni accesso alle tecnologie informatiche può essere facilmente ricondotto alla persona che lo ha effettuato;
- definire in maniera trasparente le modalità di effettuazione dei controlli e le conseguenze, anche disciplinari, di un utilizzo indebito.

Art. 2
PRINCIPI GENERALI

1. La Camera di Pavia promuove il corretto utilizzo degli strumenti informatici, della Rete Informatica e Telematica, con particolare riferimento all'uso di internet, alla posta elettronica, e del Sistema di telefonia quali strumenti utili a perseguire con efficacia, efficienza ed economicità le proprie finalità istituzionali, in un'ottica di semplificazione dell'attività amministrativa, nel rispetto dei principi e delle linee guida delineati dalla normativa vigente.
2. La titolarità dei beni e degli strumenti informatici, telematici e di telefonia è in capo alla Camera di Pavia. Tali strumenti sono messi a disposizione del personale, degli addetti che operano in outsourcing e di coloro che svolgono attività lavorativa in ambito camerale. La dotazione degli strumenti e delle risorse informatiche, telematiche e di telefonia non costituisce titolo per l'acquisizione di alcun diritto in capo ai predetti soggetti e può essere ridotta, sospesa o eliminata qualora ne sussistano le motivazioni.
3. I soggetti di cui al precedente punto 2, dopo aver ricevuto le relative istruzioni, e comunque anche sulla base dei principi di diligenza, correttezza e buona fede, sono responsabili, sotto i profili amministrativi civili e penali, del corretto uso degli strumenti informatici, telematici e di telefonia e del contenuto delle comunicazioni effettuate. Rispondono dei danni, anche all'immagine dell'Ente, che possono derivare da comportamenti illeciti.
4. La Camera di Pavia privilegia l'attività di prevenzione rispetto a quella di controllo, indicando ed attuando, in un'ottica di reciproco affidamento, appropriate misure di tutela e promuovendo misure di autotutela da parte dei fruitori, nonché assicurando la massima diffusione al contenuto del presente Disciplinare.
5. Nello svolgimento dell'attività di monitoraggio e controllo la Camera di Pavia agisce nel rispetto della normativa vigente, con particolare riguardo alla tutela dei diritti dei lavoratori e alle garanzie in materia di protezione dei dati personali, nell'osservanza dei principi di ragionevolezza, correttezza, trasparenza e proporzionalità.
6. La Camera cura l'adeguata formazione del personale sull'utilizzo degli strumenti informatici, telematici e di telefonia anche in relazione alla tutela dei dati personali.

Art. 3
DESTINATARI

1. Il presente Disciplinare si applica ai dirigenti, ai dipendenti, o a questi assimilati, ed in genere a tutti gli autorizzati ad accedere alla rete camerale e agli strumenti informatici,

telematici e di telefonia (d'ora innanzi più brevemente denominati "personale") per lo svolgimento della propria attività lavorativa.

2. Il Disciplinare regola l'utilizzo di tutti gli strumenti informatici, telematici e di telefonia a disposizione degli Uffici/Servizi, siano essi impiegati in modalità indipendente o collegati alla rete informatica camerale. Esso deve essere conosciuto e applicato da tutti i Servizi dell'Ente.
3. A tal proposito, il Disciplinare è reso sempre fruibile, tramite pubblicazione nella intranet a cui ha accesso tutto il personale ed è diffuso tramite apposito Ordine di Servizio.
4. Le prescrizioni del presente Disciplinare integrano le specifiche istruzioni impartite agli autorizzati in materia di trattamento dei dati personali ai sensi del Regolamento UE n. 679/2016 e del D.Lgs. n. 196/2003.
5. La rete informatica, telematica e telefonica comprende:
   - il complesso delle risorse infrastrutturali, nell'ambito delle quali rientra ogni personal computer, laptop, stampante, scanner e strumentazione informatica in uso presso la Camera nelle componenti hardware (tutte le componenti "fisiche" del computer, quali periferiche, parti elettriche, meccaniche, elettroniche ed ottiche) e software (i programmi e le procedure) e gli apparati elettronici collegati alla rete informatica camerale;
   - i collegamenti fissi o mobili a internet e alla posta elettronica e gli apparati elettronici necessari;
   - il patrimonio informativo digitale, che include le banche dati digitali e, in generale, il materiale e la documentazione prodotta tramite i suddetti strumenti;
   - ogni apparecchiatura telefonica in uso presso la Camera, quali telefoni fissi, mobili, cellulari.
6. La vigilanza sul rispetto del Disciplinare da parte dei destinatari è esercitata, nel rispetto della normativa vigente, dal Segretario Generale sulle aree dirigenziali e dai Responsabili di Posizione Organizzativa sui rispettivi Servizi e, nell'ambito del singolo Servizio, il controllo sugli utenti è affidato al relativo responsabile.

Sezione II

USO DEGLI STRUMENTI INFORMATICI, TELEMATICI E DI TELEFONIA

Art. 4
CRITERI GENERALI DI UTILIZZO

1. Premesso che, nell'ambito dei comportamenti da porre in essere con riferimento ai rapporti di lavoro, vigono i principi di diligenza e di fedeltà – artt. 2104 e 2105 del Codice Civile – e che gli stessi si applicano anche all'utilizzo delle risorse informatiche e telematiche, attraverso il presente Disciplinare si intende evitare che comportamenti consapevoli o inconsapevoli possano arrecare danni o creare minacce per la Camera.
2. È escluso qualsivoglia uso delle risorse informatiche e telematiche per scopi privati e/o personali, a eccezione dei casi d'urgenza e comunque a condizione che tale uso avvenga in modo non ripetuto o per periodi prolungati.
3. I soggetti che utilizzano le risorse informatiche camerali, destinatari del Disciplinare, devono rispettare la riservatezza dei dati e delle misure di accesso ai servizi e sono invitati a

segnalare al Segretario Generale, quale Responsabile dei Trattamenti dei Dati Personali, o del Responsabile per la Protezione dei Dati (RPD) eventuali violazioni della riservatezza delle quali venissero a conoscenza, nel rispetto del Modello operativo per la protezione dei dati personali – Procedura "Gestione data breach".

4. La Camera si riserva la possibilità di configurare dei filtri o dei sistemi per prevenire operazioni che non rientrano nell'attività lavorativa. A titolo esemplificativo, può prevedere sistemi che impediscono l'upload (caricamento), ovvero l'accesso a specifici siti, inseriti in una cosiddetta blacklist, e/o il download (scaricamento) di file o software che hanno determinate caratteristiche legate alla tipologia dei dati o alla loro dimensione. Queste e altre misure preventive volte a ridurre il rischio di utilizzo improprio e potenzialmente dannoso, sono espressamente raccomandate dal Garante della Privacy nella Deliberazione 1 marzo 2007, n. 13 (G.U. n. 58 del 10 marzo 2007). Ogni provvedimento verrà attuato e debitamente pubblicizzato nel pieno rispetto del Regolamento UE 679/2016 e del Codice Privacy.

Art. 5
UTILIZZO DEGLI STRUMENTI INFORMATICI

1. Gli strumenti informatici (personal computer, stampanti, ecc.), telematici (accesso ad internet, tramite collegamento fisso o mobile, posta elettronica, ecc.) e telefonici (telefono fisso, mobile, cellulare, ecc.), messi a disposizione dei dipendenti, costituiscono strumento di lavoro.
   Pertanto l'utilizzo di essi è consentito, di regola, per finalità attinenti o comunque connesse con l'attività lavorativa, secondo criteri di correttezza e professionalità, coerentemente al tipo di attività svolta e nel rispetto delle disposizioni normative e interne e delle esigenze di funzionalità e di sicurezza dei sistemi informativi.
2. Nella definizione di attività lavorativa sono comprese anche le attività strumentali e collegate alla stessa, quali ad esempio quelle che attengono allo svolgimento del rapporto di lavoro, e le attività compiute dai componenti degli Organi.
3. L'utilizzo di tali strumenti messi a disposizione non configura alcuna titolarità, da parte del lavoratore, dei dati e delle informazioni trattate, che appartengono alla Camera e ai quali l'Ente si riserva, pertanto, il diritto di accedere nei limiti consentiti dalle norme di legge e contrattuali.
4. Gli strumenti affidati devono essere custoditi e utilizzati in modo appropriato, con la massima attenzione e diligenza, essendo beni rilevanti anche ai fini della sicurezza del sistema. Gli strumenti sono configurati in modo da garantire il rispetto delle regole descritte nel presente Disciplinare e tale configurazione non deve essere modificata. Il personale è altresì tenuto a informare direttamente l'Ufficio Provveditorato e il proprio Responsabile di riferimento, nell'ipotesi di furto, danneggiamento o malfunzionamento anche parziale degli strumenti e/o del sistema.

Art. 6
UTILIZZO DELLA RETE INFORMATICA INTERNA

1. Lo sviluppo e la gestione della rete informatica interna della Camera di Pavia, che collega l'insieme dei servizi dell'Amministrazione e garantisce l'accesso e l'utilizzo della rete internet a tutte le stazioni di lavoro attestate sulla rete stessa, è affidata a InfoCamere Scpa.
2. Alla rete informatica interna possono essere collegate le stazioni di lavoro di tutti i Servizi della Camera la quale si riserva la possibilità di concedere, attraverso contratti o

convenzioni, il collegamento alla propria rete a soggetti/Enti pubblici o privati, a seguito di autorizzazione e approvazione da parte dell'Amministrazione che attesti la necessità della connessione ai fini della collaborazione. In tale ipotesi, sarà richiesto, alla predetta società InfoCamere, di creare un account per l'accesso alla rete con i privilegi minimi e necessari per effettuare l'attività prevista.

3. Tutti coloro che si collegano e utilizzano la rete camerale accettano senza alcuna riserva il presente Disciplinare.
4. Per accedere alla rete della Camera ogni utente deve essere in possesso delle credenziali di autenticazione costituite da un codice di identificazione (user-ID) e da una parola chiave (password), che vengono attribuite al momento dell'entrata in servizio e a seguito di richiesta a InfoCamere da parte del Segretario Generale.
5. Il codice per l'identificazione o codice utente è alfanumerico, formato da lettere e numeri. Per i dipendenti camerali esso è formato dalle lettere "cpv" seguite dal numero di matricola dell'utente, il tutto in minuscolo (es. cpv0101). I criteri di formazione del codice alfanumerico da assegnare agli utilizzatori esterni sono stabiliti dalla società InfoCamere in base alle distinte categorie degli utilizzatori. I codici identificativi assegnati agli utilizzatori esterni da InfoCamere sono tempestivamente comunicati alla Camera.
6. Con riferimento alla password, il sistema assegna automaticamente una password generica (es. infocam1) e, in occasione del primo accesso, sarà l'utilizzatore a inserire la sua password personale che dovrà essere modificata alle scadenze predefinite e visualizzate a schermo.
7. In caso di smarrimento o perdita di riservatezza, l'utilizzatore può richiedere la modifica della password anche prima dell'eventuale termine previsto.
8. A tutela della riservatezza, ogni utilizzatore deve dotare il proprio pc di una password nello screen saver, prevedendo il tempo di inattività pari ad almeno 5/10 minuti, se non di meno, e "vistando" la casella "ripristino con password", al fine di evitare che, qualora ci si dovesse spostare dalla propria postazione, altri soggetti possano utilizzare il pc assegnato.
9. Non è consentito l'accesso alla rete e ai vari programmi con le credenziali di identificazione di un altro utente, fatto salvo quanto previsto, in caso di assenza, nei successivi artt. 7, commi 19, 20, 21, 22, e 9, comma 11 del presente Disciplinare.
10. Ogni singolo utente, infatti, è responsabile della custodia e della vigilanza dei beni e degli strumenti che gli vengono affidati e non può invocare a propria discolpa, laddove non abbia rispettato le misure minime di sicurezza sopra indicate, la motivazione che altri soggetti in sua assenza abbiano utilizzato tali strumentazioni.
11. Nelle unità di rete, trattandosi di aree di condivisione di dati e informazioni prettamente concernenti l'attività lavorativa, non devono sostare, neanche per brevi periodi, documenti non inerenti la suddetta attività.
12. La Camera può svolgere attività di controllo regolari e/o straordinarie, nel rispetto della normativa vigente in materia di tutela della privacy.

Art. 7
REGOLE COMPORTAMENTALI

1. L'accesso alla stazione di lavoro è condizionato al corretto inserimento delle credenziali di autenticazione (nome utente e password). Per l'uso, la scelta, la modifica e la custodia delle credenziali si rinvia al successivo art. 10.
2. Ogni utente abilitato all'accesso è tenuto ad utilizzare il sistema VDI per lo svolgimento delle proprie attività lavorative in quanto:
   - il sistema VDI permette all'utente di avere un ambiente sempre configurato in modo

idoneo alle esigenze lavorative;
- tutti i dati contenuti all'interno del VDI sono sempre disponibili anche accedendo da postazioni diverse, utilizzando le proprie credenziali, e sono salvati su server dedicati che ne permettono il loro eventuale recupero;
- il sistema VDI permette inoltre il ripristino quasi immediato della postazione di lavoro qualora ci fossero problemi sulla macchina fisica.

3. In capo a ogni utilizzatore vige l'obbligo di espletare le prestazioni lavorative con comportamenti idonei a non causare danni o pericoli agli strumenti e beni mobili a esso affidati (D.M. 28 novembre 2000 "Codice di comportamento dei dipendenti delle pubbliche amministrazioni" e CCNL), comprese tutte le risorse tecnologiche e informatiche messe a disposizione dall'Amministrazione.
4. Gli utilizzatori che, per la posizione ricoperta e le funzioni svolte, si trovino a gestire documenti che contengono dati sensibili o informazioni riservate dell'Amministrazione devono adottare particolari cautele, oltre che nella custodia, anche nell'utilizzo di strumenti tecnologici come supporti magnetici rimovibili (DVD, CD, supporti USB, ecc.), al fine di evitare che il contenuto possa essere trafugato e/o manomesso.
5. Il soggetto abilitato alla predisposizione e manutenzione della postazione di lavoro - che può essere rappresentato da una società esterna a cui venga affidato l'incarico - effettua le operazioni necessarie e dota la postazione stessa di tutti gli strumenti utili allo svolgimento dell'attività lavorativa
6. Le modifiche alla configurazione delle stazioni di lavoro possono essere effettuate unicamente da soggetti espressamente e formalmente autorizzati dalla Camera. Il personale non è autorizzato a modificare il sistema neppure se si tratta della postazione di lavoro assegnata.
7. A titolo esemplificativo, ma non esaustivo, sono considerate modifiche del sistema:
   a) modificare i collegamenti di rete esistenti;
   b) usare dispositivi removibili (CD, dvd, hard disk, floppy etc.) per alterare la procedura di avvio del dispositivo e in particolare per effettuare l'avvio di un sistema operativo diverso da quello fornito dalla Camera;
   c) aprire la struttura esterna (case) dell'elaboratore e procedere alla modifica (eliminazione o aggiunta) di componenti dello stesso;
   d) installare, senza l'assistenza di personale autorizzato, un qualsiasi software, inclusi quelli scaricati da Internet, o comunque alterare la configurazione della stazione di lavoro assegnata.
8. I principi di diligenza, correttezza e buona fede prevedono anche i seguenti comportamenti:
   a) l'obbligo di non manomettere le funzionalità del collegamento alla rete camerale e di non eseguire programmi che possano danneggiare il sistema;
   b) l'obbligo di porre in essere tutte le misure di sicurezza legate alle procedure di accensione e spegnimento delle apparecchiature;
   c) l'obbligo di utilizzo dei software e dello spazio disponibile sul server per la memorizzazione dei dati concernenti l'attività lavorativa: a tal fine, si raccomanda il salvataggio dei dati per il tempo utile, ripulendo la memoria periodicamente ed evitando ridondanze e la conservazione di file obsoleti;
   d) l'obbligo di segnalare tempestivamente all'Ufficio Provveditorato e al proprio Responsabile diretto ogni anomalia o disfunzione degli hardware e dei software al fine di ripristinare il corretto funzionamento degli stessi;
   e) l'obbligo di non effettuare modifiche hardware agli apparecchi in dotazione;

f) il divieto di installare sulla stazione di lavoro software non connessi alle prestazioni lavorative e/o non dotati di licenze d'uso legali e, comunque, software anche gratuiti (freeware o shareware) non distribuiti e/o comunque non espressamente autorizzati dalla Camera;
g) il divieto di collegare alla stazione di lavoro periferiche hardware o dispositivi non messi a disposizione dall'Ente se sussiste anche il minimo dubbio che possano contenere file con virus;
h) il divieto di porre in essere azioni contrarie alle norme di legge vigenti e in generale l'obbligo di non adottare comportamenti che possano avere effetti negativi per l'Amministrazione e per l'operatività della rete camerale e degli strumenti di sua proprietà.

9. InfoCamere, nell'ambito dell'ordinaria attività di manutenzione e di gestione della sicurezza, può monitorare e controllare il corretto utilizzo della rete camerale. La Camera si riserva di assumere le decisioni che ritiene più opportune su dati e informazioni contenuti nella memoria delle apparecchiature di sua proprietà. Il tutto nel rispetto della normativa vigente
10. Per quanto concerne le periferiche (es. stampanti) e il materiale di consumo (es. carta, toner, supporti come CD e DVD), si precisa che il loro utilizzo deve essere riservato ad attività nell'ambito di funzioni istituzionali e devono essere evitati sprechi.
11. Qualora un utilizzatore ricevesse l'attribuzione di un pc portatile, quest'ultimo dovrà essere custodito con diligenza, non solo in relazione alla postazione di lavoro, ma anche in occasione di spostamenti all'esterno delle sedi della Camera e nel caso di prestazione lavorativa in modalità agile, adottando tutte le misure necessarie per evitare pericoli, danni o sottrazioni. L'utilizzatore è il responsabile del pc portatile che gli è stato assegnato.
12. E' consentito, a garanzia del raggiungimento di più elevati livelli di efficienza, il collegamento alla rete camerale, anche attraverso WI-FI, con apparecchiature non di proprietà dell'Amministrazione (notebook, palmari, smartphone, ecc), nel rispetto, comunque, del presente Disciplinare.
13. E' vietato:
    a) accedere al *Bios* delle stazioni di lavoro e impostare protezioni o password ulteriori rispetto a quelle contemplate nel che limitino l'accesso alle stazioni di lavoro stesse;
    b) caricare o detenere nelle postazioni di lavoro e/o stampare materiale di contenuto non attinente allo svolgimento dell'attività lavorativa, in particolare quando questi comportamenti interferiscano con le mansioni attribuite, ovvero aggravino i rischi connessi all'utilizzo dei relativi strumenti;
    c) in ogni caso, caricare, detenere e/o stampare materiale informatico (a mero titolo esemplificativo: testo, audio, video):
        - il cui contenuto sia chiaramente tutelato da diritto d'autore. Nel caso in cui ciò sia necessario per la propria attività lavorativa, l'utente è tenuto ad attivare preventivamente gli adempimenti previsti dalla legge;
        - il cui contenuto sia contrario a norme di legge.
14. Le cartelle presenti nel server della Camera di Pavia sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in questa unità. Su tale unità vengono svolte attività di verifica e amministrazione da parte di personale di società incaricata dalla Camera e da Infocamere.
15. I soggetti incaricati potranno in qualsiasi momento procedere alla rimozione di file o

applicazioni che riterranno essere pericolosi per la sicurezza, ovvero acquisiti o installati in violazione del presente Disciplinare sia sulle stazioni di lavoro sia sui server di rete.

16. Al fine di garantire la corretta effettuazione delle attività di backup e conseguentemente la possibilità di ripristinare i files in caso di distruzione accidentale per guasti hardware o cancellazioni involontarie, i dipendenti devono salvare i files nelle cartelle (individuali o condivise) presenti sul server e non sulla macchina fisica.
17. L'accesso alle procedure operative degli applicativi InfoCamere è prioritariamente e di norma consentito a più di un dipendente per applicativo, a garanzia della continuità dell'attività amministrativa e per evitare disservizi in caso di assenza di un dipendente abilitato, oltre che al fine di mantenere, per quanto possibile, certa e distinta l'individualità di chi accede agli applicativi utilizzati dalla amministrazione.
18. In caso di assenza di uno dei dipendenti abilitati, il procedimento già seguito dalla persona assente sarà preso in carico da altro dipendente abilitato, in modo che risulti tracciabile, riconoscibile e verificabile il suo operato.
19. Nella impossibilità di attuare i due precedenti commi (assenza di tutti gli abilitati), in deroga al principio in base al quale non possono mai essere utilizzate le credenziali di un altro dipendente, l'assente deve delegare per iscritto (anche con mail o con messaggio telefonico) un altro lavoratore ad accedere a dati e procedure del proprio personal computer se ciò si renda indispensabile e indifferibile per esclusiva necessità di operatività o sicurezza o per improrogabili necessità legate all'attività lavorativa.
20. Il lavoratore delegato accede ai dati e alle procedure su richiesta del Dirigente o del Responsabile di Servizio.
21. Ogni utente può preventivamente consegnare al lavoratore che intende delegare e al Dirigente o al Responsabile di Servizio, una busta chiusa contenente le proprie credenziali di accesso avendo cura di sostituirla ogni volta che esse vengono cambiate.
22. In caso di assenza del delegato e se ciò si renda indispensabile e indifferibile per esclusiva necessità di operatività o sicurezza o per improrogabili necessità legate all'attività lavorativa, è consentito l'uso delle credenziali di accesso direttamente al Dirigente/Responsabile. che effettuerà l'accesso informando, per iscritto, il dipendente assente, alla prima occasione utile, delle operazioni effettuate.
23. I dipendenti, onde evitare il più possibile l'applicazione della delega di cui al precedente comma 19, devono segnalare per tempo che per una certa piattaforma il soggetto abilitato ad accedervi è solo uno.

Art. 8
UTILIZZO DELLA RETE INTERNET

1. L'accesso alla Rete Internet costituisce strumento di lavoro ed è consentito, di regola, per finalità direttamente attinenti o comunque connesse all'esercizio dell'attività lavorativa. E' escluso qualsivoglia uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza o di necessità. E' in ogni caso vietato l'uso reiterato e prolungato per fini personali.
2. E' vietato entrare nella rete e nei programmi con un codice di identificazione diverso da quello assegnato. Le credenziali di accesso alla rete ed ai programmi sono segrete e vanno gestite secondo le istruzioni impartite nel successivo articolo 10.
3. E', altresì, vietato:
   a) scaricare e/o installare software non espressamente autorizzati dalla Camera di Pavia;
   b) scaricare e/o usare materiale informatico non direttamente attinenti all'esercizio dell'attività lavorativa;

c) partecipare a forum di discussione on line, a chat, utilizzare sistemi di chiamata o di video chiamata, ecc. per ragioni non direttamente attinenti o connesse all'attività lavorativa, anche utilizzando pseudonimi o nickname;
d) navigare in internet su siti contrari a norme di legge;
e) effettuare ogni genere di transazione finanziaria per fini personali;
f) installare e utilizzare strumenti per lo scambio di dati attraverso internet con metodologia *Peer to Peer* (es. eMule, kazaa, bittorrent etc.) indipendentemente dal contenuto dei file scambiati;
g) accedere tramite gli strumenti camerali alle caselle di posta elettronica personali esterne.

4. In un'ottica preventiva la Camera di Pavia ha già provveduto a predisporre un sistema informatico di filtraggio teso ad impedire la navigazione su siti web contrari a norme di legge, o considerati non sicuri. Tuttavia, la Camera si riserva di disporre ed effettuare controlli relativi al traffico web, finalizzati al rispetto del presente Disciplinare, con le modalità di cui al successivo art. 12.

Art. 9
UTILIZZO DELLA POSTA ELETTRONICA

1. La Camera di Pavia mette a disposizione di ogni lavoratore il servizio di posta elettronica, assegnando a ciascuno una casella di posta individuale per fini esclusivamente lavorativi.
2. Al fine di agevolare lo svolgimento dell'attività lavorativa, la Camera rende disponibili indirizzi di posta elettronica condivisi tra più utenti (caselle di posta istituite per singole unità organizzative) affiancandoli a quelli individuali.
3. L'indirizzo di posta elettronica messa a disposizione dalla Camera di Pavia, contraddistinto dalla presenza del nome di dominio "pv.camcom.it", costituisce uno strumento di lavoro ed il suo utilizzo è consentito unicamente per finalità attinenti o comunque connesse allo svolgimento dell'attività lavorativa.
   L'assegnatario di una casella di posta elettronica personale, rappresentata da cognome@pv.camcom.it, è responsabile del relativo uso.
   La responsabilità della casella di posta elettronica assegnata a un Servizio/Ufficio è posta in capo al relativo Responsabile.
4. E' escluso, di regola, l'uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e di necessità e comunque non in modo ripetuto.
5. La sicurezza e la riservatezza della posta elettronica sono garantite dalla necessità di disporre di idonee credenziali di autenticazione per accedere alla stessa. La password dell'account di posta elettronica è scelta e registrata dall'incaricato nel rispetto dei criteri e delle regole indicati all'art.10.
6. Al fine di un corretto utilizzo della posta elettronica è vietato:
   a) inviare o memorizzare messaggi di natura oltraggiosa, volgare, diffamatoria e/o discriminatoria, ed in ogni caso contrari a norme di legge o idonei a creare danno alla Camera o a terzi nonché messaggi a catena e/o spam;
   b) scambiare messaggi impersonando un mittente diverso da quello reale;
   c) scambiare messaggi di posta contenenti file o link a siti con contenuti illegali, violenti, o pornografici, file o materiale informatico soggetto al diritto d'autore, password e/o codici d'accesso a programmi soggetti a diritto d'autore e/o a siti internet;
   d) aprire messaggi di posta o allegati di tipo eseguibile, salvo il caso di certezza assoluta dell'identità del mittente e della sicurezza del messaggio;
   e) aprire allegati di dubbia provenienza;

f) inviare dati sensibili e personali, a esclusione di quanto previsto dalla normativa in materia di protezione dei dati personali;
g) inviare comunicazioni che comportino l'impegno contrattuale dell'Amministrazione, senza il previo consenso del proprio responsabile;
h) inviare documenti strettamente riservati senza l'autorizzazione da parte del proprio responsabile;
i) diffondere configurazioni della rete camerale, di user-ID, password, ecc.

7. I dipendenti sono inoltre tenuti ad attenersi scrupolosamente alle istruzioni in materia di sicurezza inviate periodicamente da Infocamere e/o da incaricati dall'Ente.
8. In caso di assenze programmate dal lavoro, per ferie o per qualsiasi altro motivo di assenza prolungata, è consigliabile attivare preventivamente il sistema di risposta automatica. Il messaggio di risposta predefinito deve essere personalizzato dal personale e potrà indicare l'indirizzo di posta elettronica di un altro lavoratore al quale il mittente può fare riferimento in caso di comunicazioni urgenti.
9. In caso di assenze dal lavoro non programmate, l'utente attiva da remoto, se possibile, il sistema di risposta automatica della propria casella di posta elettronica.
10. L'assegnatario di una casella di posta elettronica può delegare per iscritto un altro assegnatario a verificare, in caso di sua assenza anche non prolungata e non programmata, il contenuto dei messaggi a lui indirizzati e a inoltrare al Dirigente o al Responsabile di Servizio quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa nel caso in cui, durante la propria assenza, ciò si renda indispensabile e indifferibile per esclusiva necessità di operatività o sicurezza o per improrogabili necessità legate all'attività lavorativa. Il delegato provvede su richiesta del Dirigente o del Responsabile di Servizio. Delle attività effettuate è informato l'assegnatario assente alla prima occasione utile.
11. L'inoltro dei messaggi a un'altra casella di posta elettronica avviene, altresì, in occasione di cessazione del rapporto di lavoro ovvero nel caso di assenze di lunga durata collegate a particolari congedi quali, ad esempio, le varie forme di aspettativa disciplinate dai relativi CCNL. In questi casi si procederà anche a interrompere momentaneamente il funzionamento della casella mentre, in caso di cessazione del rapporto di lavoro la stessa verrà eliminata.

Art. 10
GESTIONE DELLE CREDENZIALI DI ACCESSO

1. L'accesso al PC, agli applicativi Infocamere e alla posta elettronica è protetto da un sistema di autenticazione che richiede l'inserimento di un codice utente (username o user-id) e di una parola chiave (password). La corretta gestione delle credenziali di accesso è fondamentale in quanto:
   - tutela l'utilizzatore, ed in generale l'Ente, da accessi illeciti, violazioni e danneggiamenti del proprio patrimonio informativo;
   - tutela il dipendente da false imputazioni, garantendo che nessuno possa operare a suo nome.
2. Per la scelta delle password devono essere rispettate le seguenti regole:
   a) utilizzare almeno **8 caratteri** (la lunghezza ideale è di almeno 10-12 caratteri);
   b) utilizzare una combinazione di numeri, lettere minuscole e maiuscole, caratteri speciali quali **$ % & (@ # § =) , : ; - _ + ^**
   c) non utilizzare parole che consentono di identificare facilmente l'utente, quali ad esempio: il nome o cognome proprio, del coniuge o dei figli, le date di compleanno o altre informazioni similari;

d) non utilizzare parole ovvie, quali ad esempio: password, pippo, pluto, 123456, ecc.;
e) cercare di non utilizzare parole reali o, eventualmente, sostituire le lettere con il loro corrispondente numerico o carattere speciale;
f) evitare di utilizzare la medesima password per l'accesso al pc, ai vari applicativi e alla posta elettronica;
g) in sede di cambio della password, non scegliere una password già utilizzata in precedenza.

3. Per la corretta gestione delle credenziali di accesso è inoltre necessario rispettare le seguenti regole:
   a) cambiare regolarmente le password: la password per l'accesso ai programmi Infocamere e alla casella di posta elettronica deve essere obbligatoriamente cambiata almeno ogni **6 mesi** e deve rispettare i criteri che vengono visualizzati durante la procedura guidata; le password per l'accesso a programmi o banche dati contenenti dati personali particolari e/o giudiziari devono essere cambiate almeno ogni **3 mesi**;
   b) cambiare sempre al primo utilizzo la password di primo accesso quando fornita;
   c) non rivelare o condividere le password con colleghi di lavoro, famigliari o amici; in caso di interventi tecnici che richiedano l'accesso attraverso gli strumenti elettronici in dotazione ai dipendenti, la password deve essere digitata dal dipendente stesso;
   d) se si tiene traccia scritta delle proprie password, queste devono essere conservate in luogo sicuro e lontano da occhi indiscreti;
   e) non utilizzare la funzione, offerta da alcuni software, che consente di salvare automaticamente la password per i successivi utilizzi dell'applicazione.
4. In caso di smarrimento o blocco della password per l'accesso ai programmi Infocamere è necessario rivolgersi al referente informatico o al suo sostituto e/o da incaricati dall'Ente in quanto abilitati ad effettuare le operazioni di reset.

Art. 11
UTILIZZO DEGLI STRUMENTI DI TELEFONIA FISSA E MOBILE

1. Gli strumenti di telefonia (sia fissa che mobile) messi a disposizione dalla Camera di Pavia costituiscono strumento di lavoro e ne è consentito l'utilizzo unicamente per finalità attinenti o comunque connesse all'esercizio dell'attività lavorativa.
2. E' escluso, di regola, l'uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza e di necessità. E' in ogni caso vietato l'uso reiterato e prolungato per fini personali.
3. I dipendenti sono responsabili del corretto utilizzo del telefono fisso loro assegnato. Al fine di evitarne l'uso improprio da parte di terzi non autorizzati, è possibile inserire un codice di "blocco tastiera" facendone espressa richiesta all'Ufficio Provveditorato.
4. I dipendenti assegnatari di un telefono cellulare sono responsabili della custodia dello stesso dal momento dell'assegnazione e fino alla restituzione. In caso di furto o di smarrimento dell'apparecchio, l'assegnatario dovrà darne immediata comunicazione all'Ufficio Provveditorato ai fini dell'immediato blocco dell'utenza e presentare formale denuncia di furto o smarrimento da far pervenire in copia all'Ufficio Provveditorato per gli adempimenti di competenza.

Sezione III
CONTROLLI E SANZIONI

Art. 12
MODALITA' DI EFFETTUAZIONE DEI CONTROLLI

1. Le attività di controllo sull'utilizzo di tutti gli strumenti informatici, telematici e di telefonia in uso presso la Camera, sono poste in essere con modalità tali da garantire alla stessa il diritto di proteggere la propria organizzazione (adottando idonee misure di sicurezza per assicurare la disponibilità e l'integrità dei sistemi informativi) nonché il diritto del soggetto controllato a non vedere illecitamente invasa la propria sfera personale, nel rispetto del diritto alla riservatezza e alla dignità come sanciti, per il personale, dallo Statuto dei lavoratori e, comunque, dalla vigente normativa sulla privacy. Tutti i trattamenti dei dati degli utilizzatori degli strumenti camerali verranno effettuati, quindi, anche in sede di controllo, nel rispetto del Regolamento UE 679/2016 e del Codice Privacy.
2. I controlli, sono effettuati con modalità conformi alle disposizioni di legge, sia per verificare la funzionalità e la sicurezza del sistema che per appurare un corretto utilizzo da parte degli utenti, rispettando tutte le procedure di informazione e consultazione delle rappresentanze dei lavoratori come previsto dai CCNL di riferimento.
3. I controlli possono essere effettuati in relazione alla navigazione (con file log che tracciano le varie attività in rete degli utenti navigatori) o sui contenuti (tramite un sistema di controllo - Proxy server).
4. La Camera di Pavia si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, di svolgere dei controlli saltuari e a campione che consentano di verificare l'effettiva conformità dell'uso degli strumenti informatici e di telefonia alle presenti prescrizioni.
5. I controlli sono effettuati da Infocamere su richiesta del Segretario Generale o del Dirigente d'Area.
6. I controlli non potranno mai svolgersi direttamente e in modo puntuale, ma dovranno preliminarmente essere compiuti, secondo il principio di gradualità nell'attività di controllo, su dati aggregati, riferiti all'intera struttura organizzativa o a sue unità operative anche attraverso specifici audit informatici.
7. A seguito di detto controllo anonimo, qualora fosse rilevata una effettiva e grave anomalia dell'attività, con un avviso generalizzato verranno invitati tutti gli utenti interessati ad attenersi esclusivamente e scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Se a detta comunicazione non dovessero seguire, nei quindici giorni successivi, ulteriori anomalie, l'Ente non procederà a ulteriori controlli. In caso contrario, verranno inoltrati preventivi avvisi, sempre su base anonima, riferiti all'unità organizzativa dalla quale provenga l'anomalia riscontrata.
8. Qualora continuino i comportamenti non conformi, sono effettuati controlli nominativi o su singoli dispositivi e postazioni specificando le motivazioni del controllo e, a seconda della gravità della violazione riscontrata, saranno applicate le sanzioni di cui al successivo articolo 13.
9. In ogni caso non sono ammessi, su base individuale, controlli casuali, prolungati, costanti o indiscriminati.
10. L'Ente inoltre non effettuerà, in nessun caso, né farà effettuare da eventuali Responsabili esterni, trattamenti di dati personali mediante sistemi *hardware* e/o *software* che mirino al

controllo a distanza dei lavoratori, ovvero a ricostruire l'attività del lavoratore, quali a titolo esemplificativo e non esaustivo:

a) lettura e/o registrazione sistematica dei messaggi di posta elettronica, ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio di posta elettronica stesso;
b) riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore, dei contenuti delle medesime, nonché del tempo di permanenza sulle stesse;
c) lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
d) analisi occulta di computer o altri dispositivi portatili affidati in uso, ovvero delle rispettive connessioni ad Internet;
e) le attività descritte, ed altre per i medesimi scopi, effettuate sulle utenze telefoniche fisse o relative a telefonia cellulare.

11. Resta sempre salvo l'obbligo dell'Ente di comunicare i *log file* o altre evidenze contenenti le prove informatiche relative ai comportamenti illeciti dei dipendenti alle Autorità Giudiziarie competenti che ne facciano richiesta secondo la normativa vigente.

Art. 13
SANZIONI

1. E' fatto obbligo a tutti i dipendenti e collaboratori della Camera Pavia di osservare le disposizione del presente Disciplinare.
2. Il mancato rispetto delle regole e dei divieti di cui al presente Disciplinare costituisce, per i dipendenti, violazione del Codice di comportamento dei dipendenti delle pubbliche amministrazioni – D.P.R. 16 aprile 2016 n. 62 - e determina, nel rispetto dei principi di gradualità e proporzionalità, l'applicazione delle sanzioni disciplinari previste dalle disposizioni di legge e dal Contratto Collettivo di Lavoro vigente, fatto salvo comunque il diritto della Camera al risarcimento dei danni eventualmente patiti a causa della condotta del lavoratore.
3. Il mancato rispetto delle regole e dei divieti del presente Disciplinare costituisce, per i collaboratori esterni, violazione degli obblighi contrattuali. In tal caso si procederà alla revoca delle autorizzazioni nonché ad ogni altra eventuale sanzione in base alla gravità dell'atto, come previsto dalle norme vigenti.

Sezione IV
DISPOSIZIONI FINALI

Art. 14
DISPOSIZIONI FINALI

1. Il presente Disciplinare entra in vigore dal giorno successivo alla sua adozione e sostituisce ed abroga eventuali procedure o disposizioni con esso incompatibili.
2. La Camera può apportare in qualunque momento eventuali modificazioni e/o integrazioni al presente Disciplinare finalizzate al perseguimento di una sempre maggiore efficienza, efficacia ed economicità nell'organizzazione dell'attività lavorativa e tali da garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi.

3. Il Disciplinare, inoltre, potrà essere modificato e/o integrato a seguito di cambiamenti nella normativa di riferimento o in ragione dell'evolversi delle tecnologie dell'informazione e della comunicazione tali da richiedere adeguamenti delle disposizioni.
4. Tali modifiche dovranno essere tempestivamente comunicate a tutti i destinatari nelle forme previste dal precedente art. 3, comma 3.