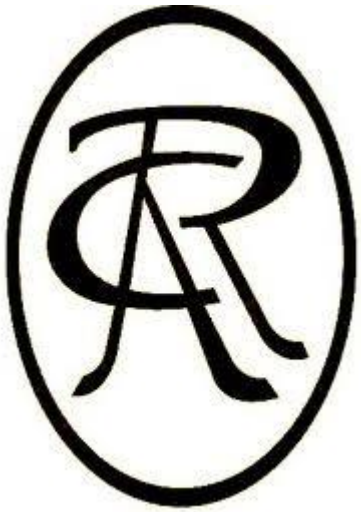
Consiglio Regionale

dell'Abruzzo



Regolamento sull'utilizzo degli Strumenti e dei Servizi Informatici

(D. Lgs. N. 196/2003)

Anno di riferimento: **2011 –** Data di redazione: **30.11.2011**

Il titolare del trattamento

_____

1 Sommario

2 Generalità

2.1 Sommario modifiche

Versione	Data	Descrizione
1.0	27/05/2010	Emissione iniziale
1.1	30/11/2011	Prima revisione

2.2 Lista di distribuzione

Dipendenti, collaboratori e Consiglieri del Consiglio Regionale dell'Abruzzo.

2.3 Riferimenti

I riferimenti legislativi e documentali del presente documento sono i seguenti:

- D.Lgs. 196/03 e relativo allegato B);
- DPS del Consiglio Regionale dell'Abruzzo.

3 Premessa

Il Consiglio Regionale dell'Abruzzo,

VISTA la "Deliberazione 1° marzo 2007, n. 13 – Lavoro: le linee guida del Garante per la posta elettronica e Internet" (Gazzetta Ufficiale n. 58 del 10 marzo 2007);

RITENUTO di doversi adeguare alle disposizioni del Garante relative all'utilizzo degli strumenti elettronici ed al possibile controllo dell'operato dei dipendenti, in equilibrato bilanciamento delle esigenze di tutela dei beni rilevanti del Consiglio e dei diritti alla riservatezza e dignità dei soggetti a cui si applica il presente regolamento;

PREMESSO che Il Consiglio Regionale dell'Abruzzo

- ha il diritto/dovere di indicare in modo chiaro e particolareggiato le modalità del corretto utilizzo degli strumenti messi a disposizione e se, in quale misura e con quali modalità possano essere effettuati eventuali controlli;

- non effettua controlli a distanza dell'attività dei dipendenti, vietati dall'art. 4 dello Statuto dei lavoratori (L. n. 300/1970), in particolare mediante sistemi hardware e software finalizzati, ad esempio:

- alla riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- alla lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati allegati, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- alla lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- all'analisi occulta di computer portatili eventualmente affidati in uso;

- privilegia, rispetto alle misure repressive, quelle organizzative e tecnologiche volte a prevenire utilizzi impropri degli strumenti, minimizzando in ogni evenienza l'uso dei dati riferibili ai dipendenti e comunque nel rispetto dei principi di necessità, pertinenza e non eccedenza, tenendo conto altresì della disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali;

adotta il presente **REGOLAMENTO**.

4 Obiettivi e finalità

L'obiettivo del presente documento è definire le politiche del Consiglio Regionale dell'Abruzzo per la corretta gestione del Sistema Informativo, sia per quanto concerne i documenti conservati su supporto informatico ed i relativi strumenti di gestione che per quelli in formato cartaceo, mediante la formalizzazione di una serie di direttive ad obbligo di tutto il personale coinvolto nel trattamento dei dati.

Il presente disciplinare, quindi, in attuazione delle linee guida del Garante per la posta elettronica e internet pubblicato nella Gazzetta Ufficiale no 58 del 10 marzo 2007 ha lo scopo principale di adottare indirizzi trasparenti, capaci di comunicare con estrema chiarezza al lavoratore le corrette modalità di utilizzo degli strumenti informatici messi a disposizione dall'Amministrazione per lo svolgimento delle mansioni attribuite, delle reti e della posta elettronica e per definire, con altrettanta chiarezza il diritto dell'Amministrazione a verificare l'uso corretto dei suddetti strumenti, ed individuare le modalità con cui I'Amministrazione esercita tale diritto.

Le scelte di base, dunque, sono orientate a prevenire usi arbitrari degli strumenti informatici o comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza dei dati senza ledere, nel contempo, il diritto alla riservatezza degli utenti, a proteggere le libertà fondamentali e la dignità delle persone.

L'Amministrazione, quale datore di lavoro, nella persona del Presidente o di un suo rappresentante (qui di seguito definito Amministrazione) adotta ogni misura volta ad eliminare la possibilità di controllo informatico, nel rispetto dell'art. 4 secondo comma dello Statuto dei lavoratori e della vigente disciplina in materia di Privacy D.Lgs. 196/03 - Codice in materia di protezione dei dati personali) che disciplinano il trattamento effettuato dai soggetti pubblici.

Il documento, sottoposto ad aggiornamenti periodici per garantire la corrispondenza con la normativa vigente e per implementazioni e modifiche derivanti dall'esperienza, sarà disponibile sul sito Intranet dell'Amministrazione (www.consiglio.loc) e nella bacheca di piano zero. Della redazione del presente disciplinare viene fatta menzione nel Documento Programmatico per la Sicurezza (DPS) di cui al D.Lgs. 196/03,art.33 ed all. B.

Nel rispetto della disciplina in tema di diritti e relazioni sindacali il documento, incluse le modifiche e implementazioni successive, viene adottato previo confronto con le OO.SS. e la RSU.

5 Campo di applicazione

Questa politica è adottata dal Consiglio Regionale dell'Abruzzo con particolare riferimento alle sedi di Pescara e di L'Aquila. Tale documento si intende applicabile a tutto il materiale di proprietà o noleggiato dall'ente ed all'utilizzo di eventuali dispositivi privati utilizzati nelle strutture dell'ente.

Le disposizioni del presente codice si applicano al presidente, ai consiglieri, al personale in forza presso i gruppi politici ed ai dipendenti oltre a tutti i soggetti autorizzati all'uso di strumenti informatici all'interno del Consiglio Regionale dell'Abruzzo.

I consiglieri ed il personale del Consiglio Regionale dell'Abruzzo sono tenuti a rispettare e far rispettare le norme ed i principi contenuti nel presente codice per l'intera durata del mandato o del rapporto di lavoro.

Il documento fa riferimento ad usi impropri dell'accesso ad internet e dell'utilizzo della posta elettronica solo in relazione a comportamenti che l'Amministrazione ritiene non conformi all'ambito lavorativo.

Per i reati commessi mediante l'uso delle tecnologie informatiche si fa riferimento alla legislazione vigente. L'Amministrazione tuttavia, deve adottare ogni possibile misura di sicurezza volta a limitare utilizzi indebiti che possano essere fonte di responsabilità per l'utente.

Per completezza, di seguito, si sintetizza la suddivisione dei reati secondo la normativa informatica.

5.1 Reati non informatici

Reati o violazione del codice civile e penale in cui il ricorso alla tecnologia informatica non sia un fattore determinante per il compimento dell'atto.

Esempi di tali tipi di reato sono l'ingiuria, le minacce e le molestie, la diffamazione,il trattamento illecito dei dati personali, la violazione della privacy, la violazione dei diritti d'autore.

5.2 Reati informatici.

Reati o violazioni del codice civile e penale in cui il ricorso alla tecnologia informatica rappresenta un fattore determinante per il compimento dell'atto.

Esempi di tali tipo di reato sono: accesso abusivo ad un sistema informatico e telematico, danneggiamento informatico, detenzione e diffusione abusiva di codici d'accesso a sistemi informatici o telematici, frode informatica, falsità in documenti informatici, diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, violazione della corrispondenza e delle comunicazioni informatiche e telematiche.

5.3 Rispetto della proprietà intellettuale e delle licenze

Tutto il personale del Consiglio regionale della Regione Abruzzo, è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale e non può, sulle apparecchiature fornite, installare hardware o software né duplicare o utilizzare software che non sia stato preinstallato , installato o comunque fornito dalla Amministrazione.

6 Uso generico e proprietà delle risorse

L'utenza, secondo i parametri definiti nel punto precedente, deve essere consapevole che i dati creati e presenti sui sistemi informatici del Consiglio Regionale dell'Abruzzo sono di proprietà del medesimo.

A causa della necessità di amministrazione e protezione della rete aziendale, l'utenza deve essere consapevole che l'Amministratore di Sistema, ed in generale, gli operatori addetti alla manutenzione dei Sistemi Informativi, durante le fasi di amministrazione e/o manutenzione della rete o in qualsiasi altro momento, possono accedere volontariamente o incidentalmente a tutti i dati presenti sui sistemi informatici aziendali.

Si ricorda che, al fine di ottemperare al D. Lgs. 196/2003 (Codice della Privacy) nei casi in cui sia indispensabile ed indifferibile accedere ai dati trattati dai singoli incaricati o agli strumenti informatici in dotazione allo stesso, sia per esigenze aziendali che per eventuali esigenze di sicurezza ed operatività dello stesso sistema informatico (ad esempio nei casi di prolungata assenza od impedimento dell'incaricato), l'ente potrà accedere ai dati ed agli strumenti elettronici mediante intervento delle figure nominate Amministratore di Sistema.

Si precisa inoltre che gli addetti alla manutenzione dei sistemi interni ed esterni e l'Amministratore di Sistema saranno incaricati mediante opportuna lettera di nomina e relativo mansionario.

7 Direttive generali sul Sistema Informativo

7.1 D. Lgs. n. 196/2003

Il D. Lgs. n. 196/2003 "Codice in Materia di Protezione dei Dati Personali" è nato con l'obiettivo di razionalizzare e semplificare la normativa esistente e di introdurre nuove garanzie per gli interessati. Esso interviene pertanto a regolare le modalità di raccolta, gestione e custodia dei dati personali (comuni e sensibili) al fine di garantire agli interessati il diritto alla protezione dei loro dati personali.

Per questo il legislatore ha ridefinito, in parte, le misure minime di sicurezza che gli enti pubblici e privati, ed i loro dipendenti/collaboratori, sono tenuti a adottare sia per il trattamento dati informatico sia per quello cartaceo. Tali misure sono individuate nell'allegato B del Codice, denominato "Disciplinare Tecnico in Materia di Misure Minime di Sicurezza".

Il presente documento individua le misure che devono essere osservate dal personale che, nello svolgimento delle proprie mansioni, gestisce quotidianamente dati personali e sensibili (indicati nel Documento Programmatico sulla Sicurezza del Consiglio Regionale).

Le istruzioni di seguito riportate, differenziate per dati personali e dati sensibili, potranno essere integrate, aggiornate e dettagliate dai Responsabili del Trattamento, previo accordo con il settore Sistemi Informativi, tramite apposite sessioni di formazione o mediante apposita documentazione (comprensiva di ulteriori specifiche sulle novità introdotte dal Codice) che verrà resa disponibile all'utenza del Consiglio Regionale dell'Abruzzo.

7.2 Misure di sicurezza generali

Omissis

7.3 Misure di sicurezza sui dati personali

Omissis

7.4 Misure di sicurezza sui dati sensibili

Omissis

8 Direttive sul Sistema Informatico

8.1 Posta elettronica

L'Amministrazione considera la posta elettronica uno strumento fondamentale di lavoro e al fine di consentire che il dipendente utilizzi tale mezzo con confidenzialità assicura la massima garanzia di segretezza per la tutela della dignità umana. Si offre quindi l'opportunità di una casella di posta personale che l'utente può utilizzare anche per fini personali e una casella di gruppo afferente all'unità organizzativa di appartenenza da utilizzare esclusivamente per attività lavorativa.

Non sono consentiti utilizzi finalizzati a divulgare contenuti illeciti o altrimenti inaccettabili, oppure finalizzati a violare i diritti legali altrui. Al dipendente è vietato intercettare, alterare impedire o interrompere comunicazioni di altri utilizzatori della rete ed installare apparecchiature idonee a tale scopo salvo che queste non siano atte a garantire le previste misure di sicurezza regionale.

Per l'assegnazione della casella di posta si utilizza il modulo allegato al presente documento e reperibile sul sito Intranet dell'Amministrazione (www.consiglio.loc).

L'Amministrazione può utilizzare e divulgare gli indirizzi della casella di posta personali e di gruppo per fini istituzionali.

8.1.1 Posta elettronica personale

La concessione di una casella di posta elettronica personale è assicurato a:

- Personale e dirigenti a tempo indeterminato e determinato
- Personale comandato da altre amministrazioni
- Consiglieri regionali.

8.1.2 Indirizzi di posta condivisa

La concessione di una casella di posta di gruppo i di struttura è consentito a livello di:

- Servizio;
- Ufficio;
- Gruppo consiliare
- Gruppi di utenti che condividono un progetto
- RSU
- Nucleo di valutazione
- Autorità indipendenti (Co.Re.Com, Difensore Civico ecc…)

8.1.3 Obblighi e facoltà dell'utente

- E' ammesso, al fine di consentire che il luogo di lavoro sia anche una opportunità di formazione sociale, l'utilizzo della casella di posta elettronica personale purché l'uso sia corretto e concentrato prevalentemente durante le pause o moderatamente durante l'attività o al di fuori dell'attività lavorativa.

- L'utente non può effettuare l'invio in massa di messaggi all'interno o all'esterno dell'Amministrazione se non per fini istituzionali e solo previa segnalazione ai responsabili della struttura informatica. La violazione di tale prescrizione comporterà una limitazione dei privilegi dell'utente. Al persistere di un utilizzo improprio la casella di posta verrà cancellata.

- La casella di posta di gruppo e di struttura può essere u1izzata esclusivamente per fini istituzionali e solo su autorizzazione del proprio responsabile.

- All'atto della cessazione del servizio o in caso di mobilità verso altre amministrazioni, il dipendente inoltra le e-mail utilizzate per lo svolgimento dell'attività lavorativa ai responsabili o colleghi della struttura di appartenenza.

- La casella di posta del dipendente non più in servizio resta attiva per 10 giorni, questo al fine di garantire un sufficiente e ragionevole periodo per il salvataggio delle informazioni personali. Decorso tale termine la struttura informatica procede a disabilitare l'utente. La struttura inforrnatica ha la facoltà, per specifiche esigenze, di prorogare il termine indicato.

- Possibilità di accesso alla posta in caso di assenza del lavoratore attraverso l'inoltro della posta o la lettura della stessa da parte di un suo fiduciario.

- I responsabili hanno I'obbligo di modificare la password di "gruppo" e di "struttura" quando un proprio collaboratore, per qualsiasi ragione,lascia la struttura di appartenenza.

8.1.4 Obblighi e facoltà dei componenti la RSU e le Organizzazioni sindacali

- I componenti della RSU e delle Organizzazioni sindacali possono effettuare l'invio di messaggi informativi mediante posta elettronica at dipendenti della Amministrazione propri iscritti o simpatizzanti. Resta ferma la facoltà del singolo dipendente di manifestare il proprio rifiuto a ricevere la posta.

8.2 Rete Internet

Nel riconoscere l'utilità dell'informazione elettronica come mezzo di soddisfacimento delle esigenze informative, formative, culturali e di comunicazione è consentito l'accesso ad Internet anche per uso personale.

8.2.1 Accesso ad internet

L'utilizzo della rete è consentito a:

- personale e dirigenti a tempo indeterminato e determinato;
- personale comandato da altre amministrazioni;
- Consiglieri regionali.

8.2.2 Obblighi e facoltà dell'utente

L' accesso ad internet per uso personale deve essere limitato, non prevalente rispetto all'attività lavofz;iva e deve essere improntato a principi generali di correttezza e responsabilità.

Poiché i contenuti delle informazioni presenti sui siti internet è propria del singolo produttore spetta all'utente selezionare criticamente i contenuti e la qualità dell'informazione.

Fermo testando le responsabilità dell'utente per i reati informatici in riferimento a comportamenti non conformi all'ambiente lavorativo non è consentito:

- Navigare in siti di carattere pornografico, pedo-pornografico
- Giocare in borsa
- Connettersi con il modem. L'uso del modem è consentito esclusivamente per la connessione a particolari siti istituzionali protetti e connessi all'attività lavorativa e solo previa verifica e autorizzazione della struttura informatica.
- Rimuovere o danneggiare le configurazioni del software
- Installare software senza l'autorizzazione della struttura informatica.

8.3 Direttive sull'uso della rete interna del Consiglio

La gestione Sistema Informatico, deve essere effettuata dallo staff preposto sotto la responsabilità degli Amministratori di sistema. Gli utenti del Consiglio Regionale dell'Abruzzo non preposti o loro collaboratori, o fornitori, o genericamente terzi, non sono autorizzati ad effettuare alcuna modifica al Sistema, neppure per quei dispositivi, Hardware e/o Software, che hanno ricevuto in dotazione dall'azienda per svolgere il proprio lavoro.

La gestione dell'Hardware è limitata per essere certi che le garanzie non vengano inavvertitamente violate e che le norme di sicurezza non vengano aggirate. L'installazione di Software è vietata per garantire la conformità dell'azienda alle leggi che riguardano i contratti di licenza.

E' vietato collegarsi ad internet attraverso collegamenti a rischio non approvati dal Servizio Sistemi Informativi e Controllo Interno.
E' vietato installare sulle proprie postazioni software non coperto da regolare licenza.
E vietato effettuare download di musica, film, e altre opere coperte da diritto d'autore.

8.4 Direttive generiche sull'uso delle postazioni informatiche

Gli utenti sono responsabili per la protezione e tutela delle postazioni informatiche a cui fanno riferimento e dei dati in esse contenuti.

Tutte le postazioni di lavoro devono essere dotate di uno "screensaver" protetto da password con attivazione automatica allo scadere di cinque minuti di inattività.

Si ricorda inoltre che non e' consentita la duplicazione dei programmi per fornirli a terzi o per uso personale al di fuori del Consiglio Regionale.

8.5 Direttive sull'uso dei computer da tavolo

Il computer da tavolo viene dato in dotazione agli incaricati sulla base ed al solo fine delle mansioni lavorative che essi svolgono; esso viene configurato, installato, posizionato e mantenuto esclusivamente dal gruppo preposto sotto la responsabilità degli Amministratori di Sistema. La sua accensione è prevista per il solo periodo lavorativo e non va lasciato incustodito da parte dell'assegnatario (o del gruppo di assegnatari) in condizioni di accessibilità. Il suo posizionamento fisico deve restare sempre quello previsto a meno di formale richiesta di spostamento, che è compito dal personale preposto. La buona cura e l'adeguato utilizzo sono responsabilità dell'assegnatario (o del gruppo di assegnatari). In caso di malfunzionamenti non è permesso in alcun modo di intervenire a soggetti diversi dal personale preposto.

8.6 Direttive sull'uso dei computer portatili

Il computer portatile viene dato in dotazione agli incaricati sulla base ed al solo fine delle mansioni lavorative che essi svolgono, nei casi in cui è prevista maggiore mobilità; esso viene configurato, installato, posizionato e mantenuto esclusivamente dal gruppo preposto sotto la responsabilità degli Amministratori di Sistema. Il computer non deve essere lasciato incustodito da parte dell'assegnatario in condizioni di accessibilità e soprattutto a rischio di furto e/o danneggiamento: ad esempio in auto, treno, aeroporto o altri luoghi in condizioni di scarsa sicurezza. La buona cura e l'adeguato utilizzo sono responsabilità

dell’assegnatario. In caso di malfunzionamenti non è permesso in alcun modo di intervenire a soggetti diversi dal personale preposto.

8.7 Direttive sulla memorizzazione delle informazioni

Ad ogni incaricato è resa disponibile una risorsa di rete raggiungibile dalla propria postazione di lavoro attraverso l’icona “risorse del computer": a questa risorsa, identificata come disco di rete, è assegnato dall’amministratore uno spazio disco per effettuare i salvataggi dei documenti.

Altri salvataggi su cartelle diverse da quella indicata non sono garantiti ai fini dell’applicazione delle misure minime di sicurezza. In caso di indisponibilità della risorsa, l’incaricato ha il dovere di informare lo staff tecnico preposto.

9 Sanzioni

Gli utenti sono direttamente responsabili sia civilmente, sia penalmente, a norma delle leggi vigenti, per l'uso improprio fatto del servizio di internet e della posta elettronica.

L'Amministrazione si riserva la facoltà, di denunciare I'utente alle autorità competenti per le attività illecite compiute durante l'attività lavorativa o con i mezzi messi a disposizione dall'Amministrazione.

Per comportamenti non conformi al presente disciplinare l'Amministrazione si riserva la facoltà di limitare o annullare i privilegi concessi al singolo dipendente.

L'utente è tenuto a risarcire l'Amministrazione per danni prodotti alle apparecchiature o alla rete in violazione delle norme vigenti e/o in violazione del presente disciplinare.

10Controlli

Il sistema Informativo e Controllo Interno, in qualità di responsabile dell'erogazione dei servizi oggetto del presente documento, adotta misure in grado di prevenire il rischio di utilizzi impropri così da ridurre il più possibile controlli successivi sugli utenti e garantendone la riservatezza delle informazioni.

10.1 Possibilità di controlli e loro gradualità

Il Consiglio Regionale ha diritto di effettuare controlli identificativi degli utenti, quando ciò sia dettato:

- da esigenze per l'esercizio o la difesa in sede giudiziaria
- da riscontri di gravi inadempienze della prestazione lavorativa
- da oggettivi indizi di commissione del reato
- da esigenze di salvaguardia della vita o dell'incolumità di terzi
- da norme specifiche di legge o dall'autorità giudiziaria.

Inoltre, le esigenze organizzative, di sicurezza ed il mancato rispetto del presente regolamento che evidenzino comportamenti anomali (evento dannoso, situazione di pericolo, rischi di responsabilità per l'ente, interferenze, rischio o danno per altri) legittima il Consiglio Regionale al controllo sull'utilizzo del web e dell'e-mail.

La verifica sui comportamenti anomali verrà effettuata con controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa (o su una specifica area).

Il controllo anonimo può concludersi con avviso generalizzato sul rilevato utilizzo anomalo degli strumenti dell'ente e con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle disposizioni impartite;

L'avviso e l'invito verranno rivolti solo all'area in cui verrà eventualmente rilevata l'anomalia.

In assenza di successive anomalie (di norma) non saranno effettuati controlli individuali.

Non saranno effettuati controlli prolungati, costanti o indiscriminati.

10.2 Conservazione dei dati

Sono memorizzate temporaneamente *Omissis* le informazioni relative all'uso degli strumenti elettronici indispensabili per le seguenti finalità:

- protezione dell'intera rete da e verso l'esterno (firewall)
- difesa della corrispondenza e navigazione informatica (antispamming/antivirus)
- controllo automatico dei contenuto dei siti (web filtering)

I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati relativi agli accessi ad Internet e al traffico telematico

Eccezionalmente la conservazione può essere protratta, per il tempo indispensabile e per le sole informazioni necessarie, in relazione:

- a esigenze tecniche o di sicurezza particolari
- all'indispensabilità dei dati rispetto all'esercizio o difesa di un diritto in sede giudiziaria
- all'obbligo di custodire o consegnare i dati per specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In ogni caso il Servizio Sistema Informativo e Controllo Interno provvederà alla custodia e controllo delle informazioni in ottemperanza all'art. 31 (Obblighi di sicurezza) del d.lgs. 30 giugno 2003 n°196 nonché a garantire la sfera di riservatezza nelle relazioni personali e professionali nel rispetto della Costituzione (artt. 2 e 41), dell'art. 2087 del codice civile e della normativa in materia di digitalizzazione dell'informazione.

10.3 Modalità di controllo

Il Servizio Sistema Informativo e Controllo Interno, nel conformarsi a principi di necessità, correttezza, pertinenza e non eccedenza, per la verifica del corretto utilizzo della posta elettronica e di internet:

- Si riserva la facoltà di effettuare controlli periodici nei log file, in conformità della legge al solo fine di garantire la funzionalità e sicurezza del sistema. I dati da elaborare verranno estratti privi di qualsiasi riferimento che possa essere ricondotto all'utente (matricola, cognome nome, indirizzo IP, MAC Address);

- elabora informazioni di tipo statistico quali accessi a banche dati, visite a siti di interesse riservandosi la facoltà di raggruppare dati per struttura per verifiche di fruibilità;

- non effettua monitoraggi sistematici delle pagine Web visualizzate dal singolo lavoratore. saltuariamente può estrarre pagine visitate dai dipendenti, prive di riferimenti che possano essere ricondotti al singolo utente, per l'individuazione di siti non correlati all'attività lavorativa da inserire nel web filtering. L'attività di monitoraggio verrà svolta esclusivamente dal personale del Servizio Sistema Informativo e Controllo Interno preposto, che sarà tenuto al rispetto del principio di segretezza;

- non consente in alcun modo la lettura della posta elettronica personale ad altri, né consente di fare copia delle stesse. Per assenze prolungate o impedimenti e nella impossibilità di inoltrare posta inerente l'attività lavorativa,un dipendente può indicare un fiduciario per la lettura della sua posta personale;

- adotta procedure per l'accesso di emergenza alla posta personale consentite esclusivamente per improrogabili necessità e solo previa autorizzazione del dirigente e/o del direttore alla presenza di un fiduciario indicato dal dipendente. Qualora il dipendente non sia nelle condizioni di poter indicare un suo fiduciario, a garanzia di inutili intrusioni nella sfera personale del lavoratore l'accesso alla casella di posta avverrà alla presenza del Dirigente della struttura informatica in qualità di Responsabile del trattamento e di Amministratore di Sistema.

Consiglio
Regionale

SERVIZIO SISTEMA INFORMATIVO E CONTROLLO INTERNO
UFFICIO INFORMATICA

Richiesta di Account di Posta Elettronica

Il sottoscritto _____, dipendente/consigliere del Consiglio Regionale dell'Abruzzo con matricola _____, chiede l'assegnazione di un account di posta elettronica nel dominio ufficiale @crabruzzo.it dell'Ente:

☐ personale *nome.cognome@crabruzzo.it*

☐ di gruppo _____*@crabruzzo.it*

☐ di struttura _____*@crabruzzo.it*

L'Aquila_____

Il richiedente

_____

☐ il richiedente dichiara di aver preso visione e di accettare il disciplinare sul corretto utilizzo della posta e di internet.

1) L'account di gruppo deve essere sottoscritto dal capogruppo o in alternativa da un consigliere del gruppo.

2) L'account di struttura deve essere richiesto dal dirigente o dal responsabile della struttura stessa