Regione Umbria
Assemblea legislativa

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3283
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

Servizio Risorse e Sistema informativo
Sezione Sistema informatico

Istruzioni operative per l'uso degli strumenti informatici e di comunicazione

(approvato con deliberazione dell'Ufficio di presidenza n. 87 del 15.02.2016 e modificato con deliberazione dell'Ufficio di presidenza n. 159 del 18.10.2016)

Regione Umbria
Assemblea legislativa

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

Servizio Risorse e Sistema informativo
Sezione Sistema informatico

Indice generale

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

Servizio Risorse e Sistema informativo
Sezione Sistema informatico

Premesso

(a). Che l'Assemblea Legislativa della Regione Umbria (di seguito il Titolare) deve conformare periodicamente le proprie operazioni di trattamento alle disposizioni del D.Lgs. 30 giugno 2003 n. 196, Codice in Materia di Protezione dei Dati Personali (di seguito Codice) anche sotto il profilo della adozione delle misure di sicurezza (Artt. 31 e ss., D.Lgs. 196/2003, e relativo Allegato B - *Disciplinare Tecnico in Materia di Misure Minime di Sicurezza*);

(b). che è interesse del Titolare adeguare alle vigenti disposizioni di legge in materia, il trattamento di dati personali correlato all'uso da parte degli utenti del dominio della posta elettronica e della rete Internet, in ottemperanza al provvedimento del 01.03.2007 del Garante per la protezione dei dati personali [doc. web. 1387522];

(c). che il Titolare, adottando istruzioni operative per l'uso degli strumenti informatici e di comunicazione, intende assicurarne la funzionalità ed il loro corretto impiego da parte degli **utenti del dominio,** definendone modalità d'uso nell'organizzazione dell'attività lavorativa ed istituzionale, tenendo conto della disciplina in tema di diritti e relazioni sindacali, ed adottando idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi e dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (artt. 15, 31 ss., 167 e 169 del Codice);

(d). che la disciplina delle modalità di utilizzo degli strumenti informatici e telematici e dei relativi controlli in funzione della loro attuazione, garantiscono sia il diritto del Titolare di proteggere il proprio patrimonio informativo, in conformitá con le vigenti disposizioni di legge, sia i diritti alla riservatezza ed alla dignità degli **utenti del dominio**;

(e). che l'utilizzo di *Internet* da parte degli utenti del domino può formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web;

(f). che i servizi di posta elettronica sono parimenti suscettibili di controlli che possono giungere fino alla conoscenza da parte del Titolare del contenuto della corrispondenza;

(g). che le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili;

(h). che alle registrazioni dei dati da ultimo menzionati avrà accesso, solo ed esclusivamente il personale autorizzato per iscritto;

(i). che usi scorretti degli strumenti informatici o telematici espongono il Titolare a rischi di responsabilità civile e penale e possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del c.c.;

(l). che il Titolare intende utilizzare i dati relativi agli accessi del personale ai propri sistemi, applicazioni, programmi, dati e transazioni per motivi di sicurezza, corretta gestione degli stessi dati e informazioni, trattamenti statistici sui *tool* in uso aggior-

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

Servizio Risorse e Sistema informativo
Sezione Sistema informatico

nati direttamente dagli utenti con dati di loro pertinenza (ad es. note spese, cartellino, orologio, etc.), corretta gestione delle risorse informatiche e per le statistiche d'uso relative ai sistemi informatici nonché per le attività relative a modifiche tecniche/operative;

(m). che i dati non saranno in alcun caso utilizzati per controlli inerenti all'attività svolta dai dipendenti, né per fini diversi da quelli dichiarati nelle presenti Istruzioni; che esulano dalla disciplina delle presenti Istruzioni i trattamenti imposti da norme di legge, nazionali ed internazionali, nonché i trattamenti difensivi derivanti da comportamenti penalmente sanzionati dalle vigenti leggi in materia;

(n). *c*he ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, con particolare riferimento ai servizi e ai programmi a cui ha accesso e ai dati trattati a fini istituzionali. Egli è inoltre responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali;

(o). che quanto riportato nelle presenti Istruzioni non esaurisce tutte le prescrizioni contenute nelle vigenti normative relative ad illeciti disciplinari, civili e penali, con particolare riferimento alle violazioni di sicurezza e ai reati informatici.

tutto ció premesso

si portano a conoscenza di **tutti gli utenti** del dominio, le istruzioni operative di seguito indicate la cui stretta osservanza costituisce preciso dovere.

Art. 1 - Ambito, finalitá entrata in vigore.

(1.1). - Le presenti Istruzioni, unitamente al definire il diritto del Titolare a verificare il legittimo uso degli strumenti elettronici di elaborazione nonché le relative modalità di verifica, disciplinano, ai fini di un corretto utilizzo degli strumenti stessi e a garanzia della sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche, le corrette modalità di accesso e di utilizzo degli strumenti informatici, di internet e della posta elettronica, da parte del personale dipendente, dei collaboratori e dei Consiglieri della Assemblea legislativa della Regione Umbria, nell'ambito dello svolgimento delle proprie mansioni e compiti.
(1.2). - Le presenti istruzioni entrano in vigore alla data della loro pubblicazione sulla Intranet dell'Ente dandone apposita comunicazione a tutti gli utenti.
(1.3). - Le presenti Istruzioni sono soggette a revisione sulla base dell'evoluzione normativa e tecnologica, nonché sulla base delle nuove esigenze di sicurezza e di azioni correttive che si dovranno eventualmente intraprendere.

Art. 2 - Definizioni

(2.1). - Ai fini del presente Regolamento, ferme le definizioni tutte di cui al Codice in materia di Protezione dei Dati Personali si intende per:

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

***Antivirus*:** programma per elaboratore con la funzione di prevenire rimuovere o limitare gli effetti provocati da virus informatici;
***Software* o programmi:** Insieme di istruzioni da utilizzarsi direttamente o indirettamente in un elaboratore al fine di realizzare un determinato risultato;
Dominio: insieme delle infrastrutture e delle risorse fisiche e logiche di proprietà del Titolare destinate all'esercizio dell'attività dell'ente individuate logicamente con il nome **cru.it;**
***Download*:** riproduzione sull'elaboratore elettronico, temporanea o permanente, totale o parziale, delle istruzioni che compongo un programma per elaboratore, ovvero dell'insieme di *byte* che compongono un *file*;
Elaboratore elettronico *(personal computer)*: macchina elettronica digitale utilizzata da un utente in grado di interpretare ed elaborare mediante appositi programmi sequenze di stati di tensione elettrica, codificati con 0 e 1 *(bit)*;
Log: qualsiasi registrazione delle attività elaborative compiute da un'applicazione che permette di ricostruire le operazioni svolte da un utente, tramite associazione logica con il codice dell'utente ovvero con informazioni sul *device* che ha operato;
Password: componente riservata di una credenziale di autenticazione associata ad una persona e a questa nota, costituita dalla sequenza di dati in forma elettronica;
***Screen Saver* o salvaschermo:** applicazione che esegue la visualizzazione di una figura o motivo in movimento che, se abilitato, si attiva automaticamente dopo un periodo predefinito di inutilizzo dell'elaboratore;
Sezione Sistema Informatico (SSI) l'insieme delle risorse destinate dal Titolare temporaneamente o permanentemente allo svolgimento di specifiche mansioni, o ricoprenti specifici ruoli tecnico-operativi, in relazione alle esigenze di organizzazione, professionalità, continuità, riservatezza e qualità dei servizi che la Sezione eroga verso gli utenti/utilizzatori.
Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento di dati personali;
Supporti di memorizzazione: supporti fisici (magnetici od ottici) destinati alla memorizzazione dei dati;

Utenti: i Consiglieri regionali e loro collaboratori, nonché i dipendenti in organico all'Ente, nonché coloro che, a vario titolo, utilizzano le risorse dei sistemi informativi in nome e/o per conto dell'Assemblea Legislativa della Regione Umbria, ovvero che sono autorizzati, in base ad uno specifico titolo (es. incarichi, convenzioni, contratti, ecc.) ad utilizzarle.

Virus informatico: *software* informatico avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

Art. 3 - Postazione di lavoro

(3.1). - Il Titolare fornisce agli utenti una postazione di lavoro, personale o condivisa, quale supporto all'attività lavorativa, in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi.

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

(3.2). - La postazione di lavoro è fornita con configurazione software ed hardware predefinita che non può essere per alcun motivo modificata da parte dell'utente.
(3.3). - Le richieste di installazione di *software* aggiuntivo o di modifica della configurazione, anche se gratuito e necessario per lo svolgimento dell'attività lavorativa, devono essere trasmesse dal Dirigente del Servizio o dal Presidente del Gruppo politico, o dal Presidente di Commissione o Comitato al Dirigente del Sistema Informatico.

Art. 4 - Regole d'uso degli elaboratori elettronici

(4.1). - Gli elaboratori elettronici *(personal computer)* utilizzati dagli utenti del dominio sono strumenti di lavoro destinati esclusivamente allo svolgimento della propria prestazione lavorativa e/o all'incarico istituzionale ricoperto.
(4.2). - Ogni loro utilizzazione non riferibile allo svolgimento di dette attività è vietata, potendo causare rischi alla sicurezza dei sistemi informativi del Titolare, oltre che disservizi ed eventuali oneri o costi aggiuntivi di manutenzione e/o riparazione.
(4.3). - L'accesso al *personal computer* è consentito solo mediante la digitazione della apposita *password* assegnata, da utilizzare ai sensi delle presenti Istruzioni. È fatto espresso divieto, salvo autorizzazione scritta, di accedere contemporaneamente con la stessa *password* da differenti elaboratori elettronici.
(4.4). - Gli elaboratori elettronici non devono essere lasciati incustoditi, dal momento che potrebbero essere utilizzati da parte di terzi senza che vi sia, poi, la possibilità di provarne un uso indebito; anche in ipotesi di allontanamento temporaneo dalla propria postazione, ciascun utente deve azionare lo *screen saver* ed attivare la relativa *password* di abilitazione. Ogni sera, prima di lasciare i locali, se non diversamente prescritto è necessario che ciascun utente spenga il proprio elaboratore.
(4.5). - Non è consentita la modifica della configurazione delle caratteristiche di sistema *hardware* e *software* predefinite sul proprio elaboratore (ivi compresa la installazione di dispositivi per la memorizzazione, comunicazione o altro: ad es. masterizzatori, *modem Wi-FI etc.*) senza preventiva, autorizzazione scritta del Titolare.
(4.6). - Non è consentito installare e/o utilizzare autonomamente programmi per elaboratore provenienti da ambienti operativi esterni al dominio del Titolare, anche se con regolare licenza d'uso, senza preventiva autorizzazione scritta del titolare del trattamento.
(4.7). - Non è consentita la riproduzione o duplicazione, la memorizzazione, neanche temporanea, di programmi per elaboratore e di *file* con contenuti protetti, in violazione delle disposizioni di cui alla, Legge 22 aprile 1941, n. 633,"Norme in materia di diritto d'Autore e d altri diritti connessi al suo esercizio" (ad es.: File musicali *MP3, Film Divx o mpeg,* ecc.).
(4.8). - Ogni utente deve prestare la massima attenzione e cautela nell'effettuare il trattamento di dati memorizzati su supporti provenienti da ambienti operativi esterni al dominio del Titolare, avvertendo immediatamente, per iscritto, il titolare del trattamento, nel caso in cui siano rilevati *virus* informatici ed attenendosi alle presenti istruzioni.
(4.9). - Il Titolare, ha facoltà, per ragioni di protezione della sicurezza dei sistemi informativi, di esaminare i dati trattati da ogni utente sia sulla propria postazione di lavoro sia sulle unità di rete utilizzate, compresi gli archivi di posta elettronica aziendali.
(4.10). - Il personale addetto della Sezione Sistema informatico, incaricato per iscritto dal titolare del trattamento, può procedere in ogni momento al controllo preventivo ed

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

alla rimozione, dai *personal computer* degli incaricati e dalle unità di rete, di ogni *programma per elaboratore* installato e/o utilizzato in violazione delle present Istruzioni e di ogni *file* ritenuto pericoloso per la sicurezza del dominio.
(4.11). - Non è consentito utilizzare strumenti *software* e/o *hardware* atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
(4.12). - non è consentita la consultazione, memorizzazione e diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
(4.13). - gli applicativi gestionali, in uso presso alcune strutture dell'Ente, sono destinati alla gestione di informazioni il cui utilizzo deve essere compatibile con la normativa vigente relativa alla privacy (D.lgs 196/2003 e successive modificazioni);
(4.14). - alla fine della giornata lavorativa, l'utente è tenuto a terminare la sessione di lavoro arrestando il sistema (spegnendo quindi il PC in dotazione) al fine di evitare l'eventuale danneggiamento delle componenti *hardware* (in caso, ad esempio, di *blackout* della rete elettrica) e in ragione di politiche di risparmio energetico; non è consentito avviare i *personal computer* con sistemi operativi diversi, incluse versioni live, da quello preinstallato;
(4.15). - Nel caso di utilizzo comune con altri utenti, e comunque prima della riconsegna alla Sezione Sistema informatico, l'utente deve provvedere alla rimozione definitiva o al salvataggio su cartelle di rete di eventuali file elaborati.

Art. 5 - Regole d'uso delle applicazioni di rete e delle stampanti

(5.1). - Le unità di rete sono aree di condivisione di dati esclusivamente inerenti l'attività lavorativa e/o istituzionale e non possono in alcun modo essere utilizzare per scopi diversi; quindi:

(a). qualunque informazione non riferibile alle predetta attività non può essere nemmeno parzialmente (o, anche solo, temporaneamente) localizzata su dette aree;
(b). le unità di rete non possono essere utilizzate per fini non espressamente autorizzati dal Titolare;
(c). non è consentito connettere in rete postazioni di lavoro se non dietro preventiva autorizzazione scritta del Titolare;
(d). è vietato condividere cartelle in rete sulla propria postazione di lavoro anche se protette da password o da elenco incaricati autorizzati, senza preventiva autorizzazione scritta del Titolare;
(e). è vietato condividere stampanti in rete o connettersi a stampanti di rete, senza preventiva autorizzazione scritta del Titolare;
(f). è vietato monitorare ciò che transita in rete;
(g). è vietata l'installazione di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne al dominio, senza preventiva autorizzazione scritta del Titolare;

(5.2). - È fatto obbligo di effettuare la stampa dei dati solo se strettamente necessaria, e di provvedere a ritirarla prontamente dai vassoi delle stampanti comuni. Si deve evitare di stampare *file* particolarmente lunghi e/o ad elevata elaborazione grafica su stampanti comuni che non ne supportano il formato; in particolare, ogni utente **è tenuto a:**

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

Servizio Risorse e Sistema informativo
Sezione Sistema informatico

(a). stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative o istituzionali;
(b). utilizzare il centro stampa per grandi volumi di stampa, per stampe a colori o per finiture particolari (es. libretti, depliant, ecc…);
(c). laddove possibile, stampare in bianco/nero e fronte/retro ed utilizzare politiche mirate al riuso di carta per la stampa di documenti in bozza;
(d). aver cura di monitorare la stampante in caso di stampa di documenti contenenti dati o informazioni riservate e preservare, limitatamente alle oggettive possibilità, la conoscibilità dei dati o informazioni ivi contenuti da parte di terzi non autorizzati.

(5.3). - E' fatto obbligo agli utenti di provvedere periodicamente, almeno ogni sei mesi, alla pulizia degli archivi mediante la cancellazione di *file* obsoleti o inutili, residenti nelle unità di rete collegate.
(5.4). - Le *password* e le modalità di accesso alle unità di rete ed alle applicazioni in esse eseguibili sono segrete, devono essere comunicate e gestite secondo le procedure impartite quindi è espressamente vietato l'utilizzo delle predette unità e delle relative applicazioni mediante accesso con credenziali assegnate ad altro incaricato.
(5.5). - Ferme le eventuali sanzioni disciplinari a carico dell'autore della violazione, il Titolare può, in qualunque momento, procedere o invitare l'utente, alla rimozione di ogni informazione o applicazione che possa compromettere la sicurezza del dominio.
(5.6). - E' in facoltà del titolare del trattamento svolgere sulle unità di rete attività di controllo e amministrazione.

Art. 6 - Norme d'uso dei *personal computer* portatili

(6.1). - L'utente è responsabile dell'utilizzo e della custodia del *personal computer* portatile (*notebook*) che gli sia stato assegnato quale strumento di lavoro, deve custodirlo in modo diligente durante gli spostamenti, in caso di allontanamento e durante l'utilizzo nel luogo di lavoro, conservando sul disco locale solamente i *file* strettamente necessari.
(6.2). - Ai *notebook* aziendali si applicano le regole di utilizzo previste per i *personal computer* connessi in rete, con particolare attenzione alla effettuazione della rimozione di eventuali *file* ivi elaborati e conservati.
(6.3). - Anche sui *notebook* è necessario verificare l'aggiornamento dell'antivirus e, nel caso, provvedere all'aggiornamento in maniera automatica collegandosi alla rete telematica del dominio**.**
(6.4). - Per collegamenti alla rete *internet* è vietato utilizzare, sui *personal computer* portatili dell'ente, abbonamenti *Internet* privati.
(6.5). - Non è consentito l'uso di *notebook* personali collegati alla rete telematica del Titolare, o alle linee telefoniche, senza preventiva autorizzazione scritta del Titolare. Anche in ipotesi in cui il Titolare autorizzi l'uso di *notebook* personali, resta ferma ed impregiudicata la responsabilità dell'incaricato quanto a titolarità dei *software* che vi abbia istallato e la liceità dei dati che vi sono contenuti ed elaborati.

Art. 7 - Uso della rete *internet* e dei relativi servizi[1]

(7.1). - L'Ente fornisce l'accesso ad *Internet* a supporto dell'attività lavorativa ivi comprese le attività che siano strumentali e connesse alla stessa e per questo se ne

1 Articolo così sostituito con Deliberazione dell'Ufficio di presidenza n.159 del 18 ottobre 2016

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

prescrive un utilizzo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi.
(7.2). Il Responsabile del Servizio competente in materia di gestione del sistema informativo, provvede, in ottemperanza al provvedimento 26 aprile 2016 dell'Agenzia per l'Italia Digitale recante “Misure minime di sicurezza ICT per le Pubbliche Amministrazioni”, a filtrare il contenuto del traffico web e bloccare i file la cui tipologia non è strettamente necessaria per l'ente ed è potenzialmente pericolosa.
(7.3). Fatto salvo quanto previsto al comma 7.2, le categorie di siti considerati correlati o non correlati con la prestazione lavorativa e/o con l'attività istituzionale, da sottoporre a revisione periodica, sono individuate dai seguenti soggetti:

(a) l'Ufficio di Presidenza per quanto riguarda i Consiglieri regionali ed i relativi collaboratori, compresi i soggetti assegnati alle strutture di supporto, agli organi di direzione politica e ai gruppi consiliari;
(b) il Segretario generale ed i Dirigenti per quanto riguarda il personale agli stessi assegnato.

(7.4). Il Responsabile del Servizio competente in materia di gestione del sistema informativo, provvede alla configurazione di sistemi o all’utilizzo di filtri che prevengano operazioni non consentite dal presente articolo.
(7.5). Se l'utente ritiene che, in ragione del funzionamento dei filtri di cui ai commi 7.2 e 7.4 , gli sia impedito l'accesso ad una risorsa correlata con lo svolgimento delle sue mansioni lavorative, può segnalare la circostanza al proprio responsabile, il quale, a sua volta, deciderà se inoltrare la segnalazione, per gli adempimenti del caso, alla Sezione Sistema Informatico via intranet tramite il “Cruscotto Digitale” oppure a mezzo e-mail all'indirizzo sicor@alumbria.it.
(7.6). - Anche i *personal computer* che sono abilitati alla navigazione in *Internet* costituiscono uno strumento di lavoro deputato in modo esclusivo allo svolgimento della attività lavorativa e/o istituzionale; quindi, ferme le responsabilità civili e penali dei singoli utenti, non è consentito:

(a). utilizzare la rete internet per fini diversi dallo svolgimento della attività lavorativa e/o istituzionale;
(b). effettuare la registrazione a servizi offerti da operatori della rete internet che non abbiano attinenza con la prestazione lavorativa e/o istituzionale;
(c). partecipare a forum, utilizzare chat line, bacheche elettroniche e registrazioni in guest books, social network, che non abbiano attinenza con la prestazione lavorativa e/o l'incarico istituzionale ricoperto, anche usando pseudonimi o nicknames;
(d). utilizzare qualsiasi software Peer to Peer (P2P);
(e). utilizzare modem privati per il collegamento alla rete internet;
(f). effettuare il download da siti internet di qualsiasi software gratuito (freeware) e shareware senza preventiva autorizzazione scritta;
(g). di modificare le configurazioni standard del browser web fornito dall’Ente;
(h). di accedere a caselle web mail di posta elettronica personale forniti da provider che non assicurano strumenti di protezione adeguati;
(i). di effettuare ogni genere di transazione finanziaria, comprese le operazioni di home/remote banking, acquisti on-line e simili, salvo i casi direttamente richiesti dal Dirigente del Servizio interessato e autorizzati dal Dirigente del Sistema Informatico, nel rispetto ed in conformità delle procedure previste dall’Ente;
(l). di effettuare ogni forma di registrazione a siti i cui contenuti non siano legati all’attività autorizzata a ciascun utente;

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

(m). di scaricare o eseguire alcun software o altro contenuto attivo, anche se gratuito, da siti Internet se non per finalità istituzionali e solo se strettamente necessario. In tal caso, il personale preposto della Sezione Sistema Informatico verificherà la provenienza e l'autenticità del software;
(n). di utilizzare siti pubblici di condivisione dei file e di archiviazione online forniti da provider che non assicurano strumenti di protezione adeguati; (o). di caricare documenti inerenti l'attività lavorativa o istituzionale su siti pubblici di condivisione, archiviazione o backup on line.

(7.7). - Il Titolare stabilisce, con apposite autorizzazioni scritte, i casi ed i soggetti cui è consentito l'utilizzo di *software* di condivisione dati o applicazioni.
(7.8). - Il Titolare stabilisce, con apposite autorizzazioni scritte, i casi ed i soggetti cui è consentito effettuare operazioni di *remote banking*, ovvero acquisti di prodotti *on line*.
(7.9). - E' facoltà dell'Ente disporre, nei limiti dei tempi di conservazione consentiti dalle vigenti disposizioni di legge, controlli a campione sui siti web visitati, in forma anonima. L'accesso ai dati di connessione, che comprendono data e ora della connessione, indirizzo IP di mittente e destinatario, è limitato al Titolare, il quale è tenuto al rispetto delle norme in materia di protezione dei dati personali. I dati di connessione sono utilizzati esclusivamente per la ricerca di eventuali errori, per garantire la sicurezza del sistema, per verificare eventuali abusi.

Art. 8 - Connettività WI-FI

(8.1). - Il dominio del Titolare dispone di connettività WI-FI tramite la quale è possibile accedere anche alla rete internet.
(8.2). - Possono accedere alla rete internet, mediante l'uso di connettività WI-FI, solo gli utenti espressamente autorizzati dal Titolare impiegando esclusivamente i dispositivi (PC, smartphone, PAD) autorizzati dalla Sezione sistema informatico.
(8.3). - Per l'accesso ad internet in modaliltà WI-FI, saranno consegnate, dal personale preposto, all'utente del dominio apposite credenziali di autenticazione che dovranno essere conservate con la massima cura, assicurandone la loro assoluta segretezza.
(8.4). - Le predette credenziali di autenticazione non dovranno essere comunicate, al di fuori dei casi in cui detta comunicazione sia autorizzata per iscritto dalla Sezione sistema informatico.
(8.5). - Qualora un incaricato intenda impiegare per l'accesso, con connettività WI-FI alla rete internet, dispositivi di sua proprietà, dovrà essere autorizzato dal Titolare previa richiesta scritta.
(8.6). - La Sezione sistema informatico, a garanzia della sicurezza informatica del dominio, potrà subordinare l'autorizzazione all'accesso alla rete internet, mediante la connettività WI-FI riferibile al dominio del Titolare, all'esistenza di specifiche caratteristiche di protezione del dispositivo di cui si richiede l'impiego, ovvero alla installazione, sul predetto dispositivo, di meccanismi di protezione adeguati a garantire la sicurezza informatica del dominio.

Art. 9 - Strumenti di protezione del dominio

(9.1). Ai sensi e per gli effetti degli artt. 31, 33 e ss. D. Lgs. 196/2003, nonché delle disposizioni del relativo Allegato B), recante *"Disciplinare tecnico in materia di misure minime di sicurezza"*, il Titolare è obbligato *a custodire e controllare i dati personali,*

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

(9.2). - In applicazione delle norme sopra ricordate, sono poste a presidio del dominio del Titolare soluzioni (*software e/o hardware*) in grado di impedire accessi non autorizzati ai dati, la diffusione di programmi malevoli, la compromissione delle capacità operative degli strumenti (ivi compresi quelli di interconnessione, impiegati durante le operazioni di trattamento dei dati personali).

(9.3). - In particolare sono operativi software c.d. FIREWALL, ANTIVIRUS, ANTISPAM, in grado di impedire le connessioni da e verso il domino del Titolare, di impedire il diffondersi dei programmi di cui all'art. 615 quinquies, c.p. (Virus, Malware) e di filtrare, sulla base di regole stabilite, i messaggi di posta elettronica indirizzati ad utenti del dominio e di assicurare il monitoraggio dei dispositivi di protezione locale, impiegati nel corso delle operazioni di trattamento.

(9.4). - L'impiego degli strumenti di cui al comma precedente è effettuato per il tramite di personale interno addetto alla sicurezza dei sistemi.

(9.5). - L'operatività delle soluzioni di cui al presente articolo da luogo, o può dar luogo, a registrazioni (evidenze) informatiche, che contengono e/o possono contenere dati personali riferibili alla condotta realizzata per il tramite degli strumenti elettronici di elaborazione, soggetti a monitoraggio ed al controllo da parte del personale preposto alle operazioni di protezione della sicurezza dei sistemi informativi.

(9.6). - Sarà in facoltà del Titolare disporre, per finalità di prevenzione ed accertamento dei reati e/o di illeciti perpetrati in danno all'Ente, attività e/o operazioni di "investigazione digitale", anche, se del caso, facendo ricorso alla necessaria assistenza delle Autorità competenti, o di personale esterno al dominio autorizzato in conformità con le vigenti disposizioni di legge.

Art. 10 - Uso della posta elettronica

(10.1). - L'Assemblea legislativa della Regione Umbria considera la posta elettronica uno strumento fondamentale di lavoro e, al fine di consentire che l'utente lo utilizzi 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/struttura afferente all'unità organizzativa di appartenenza da utilizzare esclusivamente per attività lavorativa.

(10.2). - La casella di posta elettronica certificata (PEC) e quella ordinaria sono mezzi attraverso i quali è possibile la trasmissione di dati personali. Nei casi in cui siano utilizzati quali mezzi per trasmettere dati personali a soggetti terzi, si rammenta che tale operazione costituisce comunicazione di dati personali e, come tale deve essere effettuata ai sensi dell'art. 19 del D.Lgs. n. 196/2003, oppure a riscontro di una istanza dell'interessato ai propri dati personali. L'Amministrazione ha facoltà di utilizzare e divulgare gli indirizzi della casella di posta personali e di gruppo per fini istituzionali.

(10.3). - Le caselle di posta hanno una dimensione predefinita e non estendibile. Ogni utente è tenuto a mantenerla in ordine provvedendo a ripulirla con regolarità e salvando gli allegati ingombranti.

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

(10.4). - L'Ente concede ad ogni Consigliere regionale ed Assessore regionale, una casella di Posta Elettronica Certificata (PEC). I referenti della Sezione Sistema Informatico provvedono alla formazione on-site sul corretto utilizzo della casella.
Alle Rappresentanze sindacali interne è concessa apposita casella di posta elettronica. Tra i rappresentanti sindacali viene formalmente individuato il responsabile della casella sia in termini di utilizzo che di gestione.
(10.5). - L'accesso alle caselle e-mail personale, di gruppo/struttura e PEC avviene mediante l'utilizzo di un *browser web*. In caso di esigenze particolari è possibile richiedere alla Sezione Sistema Informatico, previa richiesta del Dirigente del Servizio di appartenenza dell'utente o del Consigliere/Assessore al Dirigente del Sistema Informatico, l'autorizzazione all'installazione di specifici programmi di gestione di posta elettronica open source (es. Mozilla Thunderbird).
(10.6). - La casella di posta elettronica personale è concessa: **(a). -** al personale in servizio presso l'Ente a tempo indeterminato e determinato; **(b). -** al personale comandato da altre Amministrazioni **(c). -** ai Consiglieri regionali.
(10.7). - All'atto della cessazione dal servizio o in caso di mobilità verso altre Amministrazioni, l'utente inoltra le e-mail utilizzate per lo svolgimento dell'attività lavorativa al Dirigente della struttura di appartenenza.
(10.8). - La casella di posta dell'utente non più in servizio resta attiva per due settimane al fine di garantire un sufficiente e ragionevole periodo per il salvataggio delle informazioni personali. Decorso tale termine la Sezione Sistema Informatico procede ad eliminarla.
(10.9). - In caso di assenza programmata e prolungata (es. per ferie), al fine di garantire la continuità dell'attività lavorativa, gli utenti sono tenuti ad utilizzare un'apposita funzionalità di sistema che invia automaticamente al mittente un messaggio di risposta, avvisando dell'assenza del destinatario e indicando eventuali modalità per contattare la struttura. In caso di assenze non programmate (es. per malattia), qualora l'utente non possa attivare la predetta procedura, se necessario il Dirigente ne richiede formalmente l'attivazione al Dirigente del Sistema informatico.
(10.10). - L'assegnazione di un indirizzo di posta elettronica personale avviene contestualmente all'assegnazione delle credenziali di autenticazione in rete dell'utente. L'indirizzo di posta personale viene creato utilizzando il nome e cognome dell'utente seguito dal dominio istituzionale @alumbria.it. L'indirizzo di email personale ha, quindi, la seguente forma: nome.cognome@alumbria.it. I casi di omonimia sono gestiti distintamente.
(10.11). - La casella di posta elettronica di gruppo o di struttura è concessa a livello di: **(a). -** Servizio; **(b). -** Sezione; **(c). -** Gruppo consiliare; **(d). -** Gruppi di utenti che condividono un progetto; **(e). -** RSU; **(f). -** Nucleo di valutazione; **(g). -** Autorità indipendenti (Co.Re.Com, Difensore Civico ecc…).
(10.12). - La casella di posta di gruppo e di struttura deve essere utilizzata esclusivamente per fini istituzionali e solo su autorizzazione del proprio responsabile. Gli utenti affidatari delle credenziali di acceso alle caselle email di "gruppo" e di "struttura" hanno l'obbligo di modificare la password quando un proprio collaboratore, per qualsiasi ragione, lascia il/la gruppo/struttura di appartenenza.
(10.13). - Allo scopo di facilitare l'interscambio di informazioni relative a scopi istituzionali, è previsto l'uso delle liste di distribuzione (mailing list). Il personale preposto della Sezione Sistema Informatico verifica, almeno annualmente, la necessità

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

di mantenere attive le liste di distribuzione e, a seguito di comunicazioni da parte della Sezione Personale, gestisce l'elenco dei nominativi inseriti in tali liste.

(10.14). - Agli utenti non è consentito:

(a). utilizzare la casella e-mail personale al fine di divulgare contenuti illeciti o altrimenti inaccettabili, oppure finalizzati a violare i diritti legali altrui;

(b). effettuare l'invio in massa di messaggi all'interno o all'esterno dell'Ente se non per fini istituzionali e solo previa segnalazione ai responsabili della Sezione Sistema Informatico;

(c). superare la dimensione complessiva di 10 Megabyte degli allegati inviati con un singolo messaggio;

(d). aprire allegati contenuti in e-mail aventi mittente e/o oggetto sospetti; ciò al fine di prevenire le minacce rappresentate da software nocivi (es. virus, worm, spyware, ecc.) che potrebbero essere contenuti negli allegati delle email stesse. Tali messaggi debbono essere cancellati immediatamente o, in caso di dubbio l'utente deve contattare immediatamente la Sezione Sistema Informatico;

(e). rispondere a messaggi di presunto *spamming* (messaggi pubblicitari o delle cosiddette "catene di S. Antonio"), neppure se al momento della cancellazione della mail viene richiesta conferma di lettura dal mittente, poiché ciò consente al mittente di verificare l'effettiva esistenza dell'indirizzo di posta dell'utente;

(10.15). - Ogni comunicazione da inviarsi che abbia contenuti rilevanti, ovvero documenti da considerarsi riservati deve essere classificata con la dicitura "strettamente riservato" ovvero "riservato-personale", o da analoga dicitura. Restano impregiudicate le procedure in essere per la corrispondenza ordinaria.

(10.16). - Nel caso in cui si ricevano messaggi provenienti da mittenti sconosciuti o messaggi insoliti, occorre cancellarli senza aprirli, segnalando tempestivamente l'accaduto alla Sezione sistema Informatico.

(10.17). - Nel caso in cui si ricevano messaggi provenienti da mittenti conosciuti, ma che contengono allegati sospetti (file con estensione *.exe .scr .pif .bat .cmd*), questi ultimi non devono essere aperti, segnalando tempestivamente l'accaduto alla Sezione sistema informatico.

(10.18). - E' possibile utilizzare la ricevuta di ritorno per avere conferma dell'avvenuta lettura del messaggio da parte del destinatario.

(10.19). - I *file* da allegare ai messaggi di posta elettronica è preferibile che siano preventivamente compressi in uno dei formati *standard* (ad es.: **.zip, *.rar, *.pdf*).

(10.20). - Per la trasmissione di *file* all'interno del dominio è consentito utilizzare la posta elettronica, purché la dimensione degli allegati non superi la dimensione di 10 Mb.

(10.21). - E' obbligatorio controllare che i *file* da allegare o allegati ai messaggi di posta elettronica siano immuni da *virus*, prima dell'invio ovvero della loro esecuzione.

Art. 11 - Norme d'uso dei supporti di memorizzazione

(11.1). - Prima di essere utilizzato nello svolgimento della attività lavorativa e/o istituzionale, qualsiasi supporto magnetico (USB) od ottico deve essere sottoposto a verifica utilizzando il *software antivirus* in dotazione. In ipotesi in cui venga rilevato un *virus*, l'incaricato non deve utilizzare i supporti in questione, ed è tenuto a segnalare tempestivamente l'accaduto alla Sezione sistema Informatico.

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

(11.2). - Non è consentito riprodurre e/o installare sul proprio elaboratore elettronico in dotazione, *files* contenuti in supporti magnetici od ottici non aventi alcuna attinenza con la propria prestazione lavorativa e/o l'incarico istituzionale ricoperto.
(11.3). - Tutti i supporti magnetici od ottici riutilizzabili (USB, CD-ROM, DVD) - a maggior ragione se contenenti dati sensibili - devono essere custoditi in archivi chiusi a chiave ed essere trattati con particolare cautela onde evitare che il loro contenuto possa essere oggetto di accesso non autorizzato.

Art. 12 - Protezione *Antivirus*

(12.1). - Ogni utente è tenuto a controllare che sul proprio elaboratore sia stato correttamente istallato il *software antivirus*, verificandone quotidianamente il regolare funzionamento e controllando che le impronte virali siano aggiornate. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante *virus* informatici o mediante ogni altro *software* aggressivo.
(12.2). - Nel caso in cui il *software antivirus* rilevi la presenza di un *virus*, l'incaricato dovrà immediatamente:
(a). sospendere ogni elaborazione in corso senza spegnere il computer;
(b). scollegare il PC dalla rete ed avvertire la Sezione Sistema informatico, utilizzando la linea telefonica.
(12.3). - Ogni dispositivo contenente dati, di provenienza esterna al dominio, il cui uso è stato preventivamente autorizzato secondo quanto disposto dalle presenti Istruzioni, dovrà essere verificato mediante il programma *antivirus* prima del suo utilizzo e, nel caso venga rilevato un *virus*, il dispositivo dovrà essere consegnato alla Sezione sistema Informatico, che provvederà ad effettuare la bonifica del supporto e ad impartire le istruzioni operative del caso.
(12.4). - È attiva la specifica casella di posta elettronica denominata sicor@alumbria.it a cui inviare le segnalazioni di anomalie o problematiche di qualsiasi genere relative a *virus* e *software antivirus*.

Art. 13 - Gestione delle credenziali di autenticazione

(13.1). - Le componenti riservate *(parole chiave)* delle credenziali di autenticazione alle applicazioni ed ai servizi disponibili nel dominio, sono assegnate dalla Sezione Sistema informatico all'atto della effettuazione del primo accesso, all'incaricato viene richiesto in automatico di cambiare obbligatoriamente la parola chiave, della quale - da tale momento - diventa l'unico depositario.
(13.2). - È fatto obbligo all'incaricato di conservare le componenti riservate delle credenziali di autenticazione e qualsiasi altra informazione legata al sistema di autenticazione informatica nella massima segretezza.
(13.3). - Le parole chiave possono essere formate da lettere (maiuscole o minuscole) e numeri tenendo presente che le lettere maiuscole e minuscole hanno significati diversi per i meccanismi di riconoscimento del sistema, e devono avere una lunghezza minima di almeno 8 (otto) possono comprendere caratteri speciali quali ad esempio % & $ # ^ ?. Non possono essere utilizzate parole presenti nei dizionari di qualunque lingua o denominazioni proprie o geografiche.
(13.4). - Le parole chiave utilizzate dagli incaricati del trattamento hanno una durata massima di 3 mesi, trascorsi i quali deve farsi luogo alla loro sostituzione.

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Tel. 075.576.3314 - Fax 075.576.3344
http://www.consiglio.regione.umbria.it
e-mail: claudia.furiani@alumbria.it

Servizio Risorse e Sistema informativo
Sezione Sistema informatico

(13.5). - Salvo che non sia diversamente stabilito è fatto espresso divieto di utilizzare le proprie credenziali di autenticazione al dominio da connessioni remote.
(13.6). - La *password* deve essere immediatamente sostituita, dandone contestuale comunicazione scritta alla Sezione sistema informatico, se si abbia ragione di temere che la stessa abbia perso il carattere della segretezza. Qualora un utente venga a conoscenza della parola chiave di altro utente è tenuto a darne immediata comunicazione, in forma scritta, alla Sezione sistema informatico.

Art. 14 - Norme d'uso della linea telefonica

(14.1). - Durante lo svolgimento della prestazione lavorativa, è vietato l'uso delle linee telefoniche per fini personali. L'utente può effettuare chiamate personali, utilizzando apposito codice rilasciato dall'Ente, sempre che le medesime siano sollecitate da impellenti esigenze di breve comunicazione privata, la cui soddisfazione giova alla migliore esecuzione della prestazione lavorativa o all'adempimento dell'incarico istituzionale ricoperto e alla salvaguardia della serenità dell'ambiente di lavoro.
(14.2). - All'interno del luoghi di lavoro non è consentito l'uso di telefoni cellulari per fini estranei all'attività lavorativa.

Art. 15 - Altri apparati di comunicazione

(15.1). - Le regole di cui ai precedenti articoli si applicano, in quanto compatibili, a tutti gli apparati idonei alla comunicazione e diffusione di dati personali facenti parte del dominio.

Art. 16 - Disposizioni in materia di riservatezza nel trattamento di dati personali

(16.1). - È fatto obbligo di attenersi alle vigenti disposizioni in materia di tutela della riservatezza rispetto al trattamento dei dati personali e di misure minime di sicurezza di cui al D. Lgs. 196/2003 e relativo Allegato B.

Art. 17 - Sanzioni disciplinari per mancata osservanza delle Istruzioni Operative

(17.1). - Il mancato rispetto di quanto disposto dalle presenti Istruzioni, oltre che con le sanzioni indicate alla lettera (i) delle premesse che precedono che forma parte integrante e sostanziale delle presenti Istruzioni, costituisce infrazione disciplinare ed è perseguibile con le relative procedure nonché con le azioni civili o penali consentite.
(17.2). - Nello specifico, le infrazioni alle disposizioni delle presenti Istruzioni, a seconda della gravità dei fatti, possono essere punite con il richiamo verbale, con il richiamo scritto e con la multa in conformità al vigente contratto collettivo di categoria al quale espressamente si rinvia per tutto quanto in questa sede non richiamato.