CITTA' DI ALTAMURA

Città Metropolitana di Bari

SETTORE II

BILANCIO - FINANZA – PROGRAMMAZIONE

Servizio CED

REGOLAMENTO PER L'UTILIZZO DELLA DOTAZIONE INFORMATICA

CITTA' DI ALTAMURA
(Prov. di Bari)
1513 R.A.
Atto depositato nella Segreteria Comunale
dal 23-08-2016 al 07-09-2016
Altamura, li 23 AGO 2016
Il Capo Servizio Segreteria
Dott. Carlo Carrera

Sommario

Art 1. Campo di applicazione

1. Il presente Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori del Comune a prescindere dal rapporto contrattuale con lo stesso intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.) ed, inoltre, agli amministratori dello stesso (componenti dell'organo esecutivo, consiglieri comunali, ecc.) ed ai componenti di organi di controllo interno (revisori dei conti, componenti del Nucleo di Valutazione, ecc.) che utilizzano in maniera, anche occasionale, dotazioni informatiche e/telematiche del Comune.
2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche:
    a. per "utente" deve intendersi ogni persona fisica in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento";
    b. per "amministratore di sistema" la una figura professionale che si occupa dei problemi inerenti la gestione e manutenzione degli impianti di elaborazione dati o di sue componenti e 'interconnessione delle strutture di elaborazione dati nella/e rete/i di computer del Comune.

Art 2. Individuazione e compiti dell'amministratore di sistema

1. L'amministratore di sistema, di seguito "amministratore", è individuato nel Capo Servizio CED dell'Ente.
2. L'amministratore stabilisce, realizza e verifica le politiche e i protocolli per l'accesso alle strutture di sistema e si occupa della configurazione della gestione dei router, degli switch, dei proxy, dei firewall e di tutti i dispositivi comunque connessi alla rete.
3. I principali settori di competenza nell'ambito dell'amministrazione di sistema sono:
    i. gestione e manutenzione degli impianti di elaborazione dati o di sue componenti;
    ii. sicurezza nella gestione e conservazione dei dati informatici;
    iii. progettazione, sviluppo, realizzazione, verifica e controllo dei sistemi di connessione LAN e WAN.;
    iv. progettazione e design di sistema;
    v. gestione di sistema;
    vi. installazione e rimozione hardware.

4. Per le sedi distaccate del Comune, le competenze di amministratore di sistema possono essere attribuite, con atto formale del Dirigente del Settore competente, ad altro dipendente in possesso di adeguato profilo e competenze professionali, ovvero estemalizzate ad azienda specializzata nel settore, che in ogni caso operano di concerto con il Capo Servizio CED.

Art 3. Utilizzo del Personal Computer

1. Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa ovvero al ruolo istituzionale ricoperto è vietato, perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il Personal Computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

2. Il Personal Computer dato in affidamento all'utente permette l'accesso alla rete del Comune di Altamura solo attraverso specifiche credenziali di autenticazione, come meglio descritto al successivo punto 3 del presente Regolamento.

3. L'amministratore o suo delegato sono autorizzati a compiere interventi nel sistema informatico comunale, diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware etc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti n° 7.4 e 8.1, potranno anche comportare l'accesso in qualunque momento, previa comunicazione all'utente della necessità dell'intervento stesso, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'ente, si applica anche in caso di assenza prolungata od impedimento dell'utente.

4. L'amministratore o suo delegato hanno la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

5. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dall'amministratore o suo delegato per conto dell'Ente, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso Ente a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

6. Salvo preventiva espressa autorizzazione dell'amministratore o suo delegato, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, smartphone, Internet Key...).

7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'amministratore o suo delegato nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto n° 9 del presente Regolamento relativo alle procedure di protezione antivirus.

8. Non è consentito collegare alla rete del Comune di Altamura Personal Computer, Pc Portatili o Smartphones e, più in generale, qualsiasi dispositivo Hardware senza l'autorizzazione dell'amministratore o suo delegato. Eventuali acquisti di personal computer devono essere necessariamente comunicati al suddetto ufficio che provvederà a predisporre l'installazione e la configurazione degli stessi.

Art 4. Gestione ed assegnazione delle credenziali di autenticazione

1. Le credenziali di autenticazione per l'accesso alla Rete Comunale vengono inizialmente assegnate dall'amministratore o suo delegato e successivamente resettate dal dipendente stesso secondo criteri prestabiliti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal'amministratore o suo delegato, associato ad una parola chiave (password) riservata e creata dall'incaricato che dovrà essere memorizzata, custodita con la massima diligenza, non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'amministratore o suo delegato.

3. La parola chiave deve essere formata da 8 o più caratteri appartenenti ad almeno tre delle seguenti quattro categorie: lettere maiuscole, lettere minuscole, numeri, caratteri speciali, anche in combinazione fra loro e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

4. La password di accesso di ciascun incaricato sarà automaticamente resettata ogni tre mesi. In base a tale procedura automatica, l'incaricato, mediante avviso a video, dovrà inserire ogni 3 mesi una password nuova, diversa dalla precedente.

5. L'utente potrà richiedere la modifica della parola chiave all'amministratore o suo delegato, per decorrenza del termine sopra previsto e/o in caso di perdita della riservatezza.

Art 5. Utilizzo della Rete

1. Per l'accesso alla rete del Comune di Altamura ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione.

2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente di un altro operatore. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

3. La presenza di cartelle di sistema condivise sono da considerarsi strumento di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia dei dati salvati su cartelle condivise, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante. E' fatto divieto salvare files musicali, video e similari sul Pc in dotazione dell' Ente.

4. I dischi o altre unità di memorizzazione locali (es. disco C:/ del proprio PC) non sono soggette a procedure automatizzate di salvataggio dati. La responsabilità del salvataggio dei dati eventualmente ivi contenuti è pertanto a carico del singolo utente, il quale sarà tenuto a copiare almeno settimanalmente, tutti i files di lavoro sul server centrale, in apposita cartella.

5. L'amministratore o suo delegato possono in qualunque momento, previa comunicazione all'utente, procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di sistema.

Art 6. Utilizzo e conservazione dei supporti rimovibili

1. Eventuali supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi.

2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare l'amministratore o suo delegato e seguire le istruzioni da questo impartite.

3. E' vietato l'utilizzo di supporti rimovibili per fini personali.

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

5. L'utente è tenuto ad effettuare la scansione antivirus delle chiavi di memoria USB prima dell'utilizzo.

Art 7. Utilizzo di PC portatili

1. L'utente è responsabile del PC portatile assegnatogli dal Servizio CED e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nei luoghi di lavoro.

2. Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

3. I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

4. Tali disposizioni si applicano anche nei confronti di incaricati esterni.

5. E' vietato connettersi alla rete comunale attraverso qualsiasi dispositivo personale (PC portatile, smart phone, ecc.) non preventivamente autorizzato dall'amministratore o suo delegato.

Art 8. Uso della posta elettronica

1. La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

2. È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

   i. l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
   ii. l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
   iii. la partecipazione a catene telematiche. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

3. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

4. È obbligatorio porre la massima attenzione nell'aprire i file allegati alle e-mail (attachment) prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

5. Nel caso in cui un utente di posta si assenti per più giorni (p.es. per malattia), sarà consentito al superiore gerarchico dell'utente o comunque, sentito l'utente, a persona individuata dall'Ente, accedere alla casella di posta elettronica, al fine di garantire la continuità del Servizio lavorativo e comunque nel rispetto del principio di necessità e di proporzionalità.

6. L'amministratore o suo delegato, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 2.3.

Art 9. Navigazione in Internet

1. Il PC assegnato all'utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa all'interno dell' Ente.

2. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare Internet per:
   - l'upload o il download di software gratuiti (freeware) e shareware;
   - l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica);
   - l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati e comunque nel rispetto delle normali procedure di acquisto;
   - ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
   - la partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;
   - l'accesso a social media (Facebook, Twitter, YouTube ecc.), salvo che l'accesso avvenga da profili istituzionali, attivati dall'URP, nel rispetto delle indicazioni contenute nel Vademecum "Pubblica amministrazione e social media" –anno 2011 del Formez.

3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Comune di Altamura rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che impedisce determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list dinamica.

4. Gli eventuali controlli, compiuti dall'amministratore o suo delegato, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 1 mese, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Ente.

Art 10. Protezione antivirus

1. Il sistema informatico del Comune di Altamura è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.

2. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto all'amministratore o suo delegato.

3. Ogni dispositivo magnetico di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus in dotazione prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà prontamente scollegare il dispositivo esterno e segnalare l'accaduto al'amministratore o suo delegato.

Art 11. Osservanza delle disposizioni in materia di Privacy

1. Gli utenti sono obbligati ad attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza previste, dal D.Lgs. n. 196/2003.

2. In particolare, ogni utente assume il ruolo di incaricato del trattamento ai sensi dell'art. 30 dello stesso Codice e, pertanto, è tenuto a:
   i. attenersi alle disposizioni impartite dal Responsabile del trattamento;
   ii. rispettare i principi di pertinenza, stretta necessità, non eccedenza rispetto alle finalità perseguite, correttezza nel trattamento dei dati personali;
   iii. effettuare la raccolta, l'elaborazione, la registrazione di dati personali esclusivamente per lo svolgimento delle proprie mansioni;
   iv. accedere alle banche dati come indicate anche oralmente dal Responsabile;
   v. non asportare supporti informatici o cartacei contenenti dati personali di terzi senza autorizzazione;
   vi. non diffondere i dati personali trattati in ragione delle proprie funzioni d'ufficio;
   vii. in caso di archivi, vigilare sulla corretta consultazione da parte di personale comunque autorizzato alla stessa;
   viii. utilizzare il computer assegnato con la massima diligenza.

Art 12. Accesso ai dati trattati dall'utente

1. E' facoltà dell'Ente accedere direttamente, esclusivamente tramite l'amministratore o suo delegato e nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telematico, esclusivamente per le seguenti finalità:
    i. motivi di sicurezza del sistema informatico;
    ii. motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.)
    iii. controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.).

2. Sono vietati accessi con finalità di controllo dell'attività lavorativa.

Art 13. Sistemi di controlli graduali

1. In caso di anomalie, l'amministratore o suo delegato effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti del'area in cui è stata rilevata l'anomalia, si evidenzierà l'utilizzo irregolare degli strumenti informatici e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

2. In nessun caso potranno essere compiuti controlli prolungati, costanti o indiscriminati.

Art 14. Sanzioni

1. È fatto obbligo a tutti gli utenti ed all'amministratore ed ai suoi delegati di osservare le disposizioni portate a conoscenza con il presente regolamento.

2. Il mancato rispetto o la violazione delle regole di cui al presente Regolamento è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari, nonché anche per gli altri utenti con azioni risarcitorie previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

Art 15. Entrata in vigore del regolamento e pubblicità

1. Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.

2. Copia del presente regolamento sarà notificata via PEC dal Servizio CED a tutti gli utenti della rete informatica comunale, nonché permanentemente pubblicata sul "Portale del dipendente" ed, altresì, affissa sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori.