COMUNE DI NURRI

Provincia di Cagliari

Disciplinare interno sulle norme comportamentali per l'accesso ai sistemi ed alle risorse informatiche, per la gestione della navigazione in Internet e della posta elettronica dell'Ente.

Approvato con deliberazione della Giunta comunale n. 41 del 02.08.2013

Il presente Disciplinare, adottato con Deliberazione della Giunta Comunale, tiene conto delle indicazioni contenute nella Deliberazione del Garante per la protezione dei Dati personali del 1 Marzo 2007 n° 13, recante le "Linee guida del Garante per la gestione della posta elettronica e la navigazione Internet" ed ha per oggetto i criteri e le modalità operative per l'accesso ai sistemi ed alle risorse informatiche, per la gestione della navigazione in Internet e della posta elettronica da parte dei dipendenti dell'Ente e di tutti gli altri soggetti che, a vario titolo, prestano servizio o attività per conto e nelle strutture del Comune (es. tirocinanti).

Definizioni

Titolare del trattamento dei Dati: secondo quanto previsto dall'art.28 del D.Lgs. 196/03 "quando il trattamento è effettuato da una persona giuridica, da una Pubblica Amministrazione o da qualunque altro Ente, titolare del trattamento dei Dati è l'entità nel suo complesso".

Il provvedimento a carattere generale del garante per la protezione dei Dati Personali, del 14 Giugno 2007 (G.U. N°161 del 13 Luglio 2007), recante le "Linee guida in materia di trattamento di Dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico", precisa definitivamente che in ambito pubblico "per individuare il titolare del trattamento Dati occorre far riferimento all'amministrazione o Ente centrale o locale nel suo complesso, anziché a singole articolazioni interne o alle persone fisiche che l'amministrano o la rappresentano (esempio presidente o direttore generale).

Responsabile del trattamento dei Dati: secondo quanto elencato nell'art. 4, comma 1 lett. g) del D.Lgs. 196/03 per responsabile del trattamento si intende "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro Ente, associazione od organismo preposti dal titolare al trattamento di Dati personali".**Incaricati del trattamento dei Dati:** secondo quanto enunciato nell'art.4, comma 1 lett. h) del D.Lgs. 196/03 per incaricati del trattamento si intendono "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".

Utente Internet: persona, all'interno dell'Ente, autorizzata ad accedere al servizio di navigazione in Internet.

Utente e-mail (posta elettronica): persona, all'interno dell'Ente, autorizzata ad accedere al servizio di posta elettronica attraverso l'utilizzo di caselle e-mail.

Internet Service Provider: azienda che fornisce il servizio Internet all'Ente (esempio telecom, tiscali, vodafone).

Postazione di Lavoro: personal computer collegato alla rete locale tramite la quale l'utente accede ai Servizi ed ai Dati da gestire.

Log: archivio dei tracciati sulle attività di consultazione in rete locale e non.

1 CAPO 1: UTILIZZO DELLA POSTAZIONE DI LAVORO

1.1 La postazione di lavoro affidata al dipendente deve essere utilizzata strettamente per attività lavorative ed ogni utilizzo differente può contribuire a creare dei disservizi, inoltre potrebbe insinuare minacce alla sicurezza dei Dati trattati dall'Ente. Tutti i dipendenti devono custodire la propria postazione di lavoro in modo diligente, segnalando per tempo ogni anomalia riscontrata e/o guasto al proprio responsabile di Area.

1.2 L'accesso a ciascuna postazione è protetto da credenziali di autenticazione che risiedono sul Server di Dominio, tali credenziali sono costituite da user ID e password le quali sono conosciute esclusivamente dall'utente.

1.3 Le credenziali di autenticazione devono essere gestite attenendosi alle seguenti istruzioni:

1.3.1 La password deve essere costituita da almeno otto caratteri alfanumerici di cui almeno tre differenti (scelti tra lettere minuscole, maiuscole, numeri e caratteri speciali)

1.3.2 La password deve essere autonomamente sostituita dall'utente (policy impostata lato Server di Dominio) al primo utilizzo e successivamente modificata con cadenza almeno semestrale.

1.3.3 La password non deve contenere riferimenti diretti o indiretti agevolmente riconducibili all'utente stesso.

1.3.4 La password deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi per nessuna ragione.

1.3.5 L'utente è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare.

1.3.6 Le credenziali di autenticazione individuali per l'accesso alle applicazioni non devono mai essere condivise con altri utenti. Se un utente necessita di trattare gli stessi Dati e/o le stesse procedure dovrà richiedere delle credenziali personali al titolare del trattamento, che a sua volta le

chiederà all'Amministratore di Sistema, persona autorizzata a creare le dovute credenziali di autenticazione necessarie.

1.3.7 L'elenco delle password che permettono l'accesso al personal computer di tutte le postazioni dovrà essere depositato presso l'Ufficio Segreteria – Affari Generali dell'Ente in busta chiusa e conservato in luogo sicuro e riservato.

1.4 Il dipendente preso atto che la conoscenza della password da parte di terzi consente agli stessi l'accesso all'elaboratore, l'utilizzo dei relativi servizi in nome dell'utente titolare e l'accesso ai Dati cui il medesimo è abilitato, con possibilità di gestione degli stessi, si impegna a:

1.4.1 Non consentire, una volta superata la fase di autenticazione, l'uso della propria postazione di lavoro a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a Internet e ai servizi di posta elettronica;

1.4.2 Non utilizzare credenziali (user ID e password) di altri utenti, nemmeno se fornite volontariamente o di cui si sia venuti a conoscenza casualmente;

1.4.3 Mantenere la corretta configurazione del proprio PC non alterando le componenti hardware e software predisposte, né tanto meno installando dei software non autorizzati.

1.5 L'utente è civilmente responsabile di qualsiasi danno arrecato al Comune, e/o a terzi in violazione di quanto espressamente previsto dalla norma e di quanto indicato nel presente disciplinare.

L'utente può essere chiamato a rispondere, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e la sua password, con particolare riferimento all'immissione nella rete Comunale di contenuti critici atti ad offendere l'ordine pubblico ed il buon costume, così come definiti dalla giurisprudenza più recente.

La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dal vigente Contratto Collettivo di Lavoro, rimanendo ferma ogni ulteriore forma di responsabilità penale.

1.6 Non è consentito installare autonomamente software provenienti

dall'esterno senza la preventiva autorizzazione dell'Amministratore di Sistema dell'Ente.

1.7 Nel caso di necessità di acquisto di programmi, di applicativi e procedure di pertinenza esclusiva di una o più Aree, sarà necessaria l'autorizzazione preventiva da parte dell'Amministratore di Sistema per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa del SIC (Sistema Informatico Comunale).

1.8 Non è consentito ai dipendenti modificare le impostazioni sulla scheda di rete LAN e neppure sul browser di navigazione, salvo esplicita autorizzazione dell'Amministratore di Sistema.

1.9 Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (masterizzatore, modem, ecc) se non con l'espressa autorizzazione dell'Amministratore di Sistema, previa richiesta scritta da parte del Responsabile del trattamento dei Dati dell'Area cui è assegnato l'elaboratore.

1.10 Ogni dipendente deve prestare la massima attenzione ai supporti di memorizzazione di origine esterna onde evitare di scaricare, anche inconsapevolmente, virus e/o qualunque codice maligno.

1.11 Non è assolutamente consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza politica o sindacale.

1.12 E' assolutamente vietato copiare, scaricare e mettere a disposizione di altri materiale protetto da copyright (files musicali, filmati ecc) di cui l'Ente non abbia acquisito i diritti.

2 CAPO 2: NAVIGAZIONE IN INTERNET

2.1 La postazione collegata ad Internet costituisce uno strumento necessario allo svolgimento dell'attività lavorativa, di conseguenza **è proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.**

2.2 Ciascun dipendente è direttamente e personalmente responsabile dell'uso del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta e delle informazioni che vi immette.
2.3 E' vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili, salvo i casi espressamente autorizzati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure assegnate.

2.4 E' vietata ogni forma di registrazione a siti o mailing list i cui contenuti non siano legati allo svolgimento delle attività lavorative assegnate.

2.5 E' vietata la navigazione in siti da cui sia possibile evincere le opinioni politiche, religiose, filosofiche e sindacali o le abitudini sessuali dell'utilizzatore, non è consentito inoltre visitare né tanto meno memorizzare documenti dal contenuto oltraggioso, discriminatorio che offendono il comune senso del pudore.

2.6 Il dipendente può navigare liberamente su tutti i siti Internet salvo avere la responsabilità di visitare siti consoni all'attività strettamente lavorativa.

3 CAPO 3: GESTIONE DELLA POSTA ELETTRONICA

3.1 L'utilizzo della posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate nel presente disciplinare, ai quali il Comune assegna una casella email di posta personale e/o di servizio.

3.2 La casella di posta istituzionale è uno strumento di lavoro che deve essere quindi utilizzato esclusivamente per esigenze connesse all'attività lavorativa, non sono ammessi utilizzi diversi o privati dell'indirizzo, conseguentemente i dipendenti ai quali è assegnata sono responsabili del corretto utilizzo della stessa.

3.3 Si evidenzia che, esclusi i casi in cui sia possibile avvalersi di una utenza di posta elettronica certificata unitamente alla apposizione della firma digitale sul documento trasmesso, i sistemi di posta elettronica non consentono di garantire circa la riservatezza delle informazioni trasmesse. Per questa ragione, si raccomanda ai dipendenti di non inoltrare informazioni e Dati classificati come "sensibili" ovvero "giudiziari e/o inerenti la salute" ai sensi dell'art. 4, comma 1, lettere d, e del D.Lgs. 196/03.

3.4 E' assolutamente vietato l'utilizzo di posta elettronica istituzionale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività svolta per l'Ente, salvo diversa esplicita autorizzazione in tal senso.

3.5 E' vietato utilizzare il servizio di posta elettronica istituzionale per inoltrare catene telematiche, petizioni, giochi, scherzi, barzellette e altre forme di email che non abbiano attinenza con l'attività svolta.

3.6 E' vietato utilizzare tecniche di mail spamming cioè invio massiccio di comunicazioni a liste di utenti non istituzionali, è parimenti vietato, allegare al testo delle comunicazioni materiale potenzialmente insicuro (programmi eseguibili, macro, script ecc.).

3.7 Al fine di recepire le linee guida dettate dal Garante per la protezione dei Dati personali in materia di posta elettronica nel rapporto di lavoro, l'Ente

provvederà a mettere a disposizione di ciascun dipendente apposite funzionalità di sistema, che consentano di inviare automaticamente, in caso di assenza dal Servizio dell'utente, messaggi di risposta che avvisano il mittente dell'assenza del destinatario, individuando eventualmente altre modalità di contatto con la struttura.

4 CAPO 4: MONITORAGGIO E TRACCIABILITÀ

4.1 Il Comune può avvalersi di sistemi di controllo per il corretto utilizzo degli strumenti di lavoro (che consentono indirettamente un controllo a distanza dell'effettivo adempimento della prestazione lavorativa e determinano un trattamento di Dati personali riferiti o riferibili ai lavoratori) esclusivamente nel rispetto di quanto previsto dal Provvedimento del Garante per la protezione dei Dati personali del 1 Marzo 2007 n° 13, di quanto disposto dagli artt. 2 e 15 della Costituzione, dall'art. 616, quarto comma, c.p. e dall'art. 49 del Codice dell'amministrazione digitale.

4.2 In particolare l'Ente, nell'effettuare controlli sull'uso degli strumenti elettronici, eviterà un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

4.3 Le comunicazioni effettuate attraverso posta elettronica sono riservate, conseguentemente il contenuto non può in nessun caso essere oggetto di alcuna forma di verifica, controllo o censura da parte del Comune, dell'internet provider o da parte di altri soggetti.

4.4 Le attività sull'uso di Internet vengono automaticamente registrate in forma elettronica attraverso i LOG di sistema. Il trattamento dei Dati contenuti nei LOG, può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.

4.5 I Dati personali contenuti nei LOG possono essere trattati esclusivamente in via eccezionale nelle ipotesi di seguito elencate:

4.5.1 Rispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;

4.5.2 Richiesta dell'amministratore di Sistema, limitatamente al caso di utilizzo anomalo degli strumenti informatici da parte degli utenti di una specifica Area (rilevabile esclusivamente dai dati aggregati) reiterato nel tempo.

4.6 I Dati contenuti nei LOG sono mantenuti per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a 90 (novanta) giorni e sono periodicamente cancellati automaticamente dal sistema.

4.7 I Dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi e di controllo del rispetto delle licenze regolarmente acquistate.