CITTA' DI BARONISSI

PROVINCIA DI SALERNO

Approvato con delibera di G.C. n. 153 del 10/05/2017

Sistema Informativo Comunale

Disciplinare per il corretto utilizzo degli strumenti informatici,della rete informatica e telematica e del sistema di telefonia

Introduzione

La realtà organizzativa del Comune di Baronissi si caratterizza per l'uso diffuso delle tecnologie informatiche che, se da un lato ha consentito l'introduzione di efficienti tecniche di gestione dei servizi, dall'altro ha dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti ai dipendenti per lo svolgimento delle proprie mansioni.

In questo senso, viene fortemente sentita la necessità di porre in essere adeguati sistemi di controllo e regole per l'utilizzo di tali strumenti in modo da evitare gli usi scorretti che, oltre ad esporre l'ente stesso a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli articoli 2104 e 2105 del codice civile e dall'articolo 23 del CCNL. e dalla Circolare AGID 17 marzo 2017 n. 1/2017 – G.U. n. 79 del 4/4/2017 "Misure Minime di Sicurezza ICT per le PA" da adottare al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi.

Il disciplinare evidenzia le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti, in particolare alla luce degli obblighi previsti dalle normative vigenti e relative all'adozione delle misure minime di sicurezza per il trattamento dei dati personali.

I criteri qui individuati sono finalizzati a garantire la custodia e il controllo dei dati personali oggetto di trattamento al fine di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza e in relazione alle conoscenze acquisite in base al progresso tecnologico, alla natura dei dati e alle specifiche caratteristiche del trattamento, i rischi di:

- distruzione o perdita anche accidentale dei dati stessi;
- accesso non autorizzato;
- utilizzo improprio delle strumentazioni;
- trattamento non consentito o non conforme alle finalità della raccolta.

I principi contenuti nella presente policy si applicano all'interno del Comune di Baronissi ovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali nella responsabilità del Comune di Baronissi.

SOMMARIO

Riferimenti

- D.lgs. n. 196 del 30/06/2003 – Allegato B
- Linee guida del Garante per posta elettronica e Internet (G.U. n. 58 del 20 marzo 2007)
- Utilizzo sul luogo di lavoro di Internet e della casella di posta elettronica istituzionale, Direttiva 02/2009 del Ministro per la Pubblica Amministrazione e l'Innovazione
- Uso della Posta Elettronica Certificata nelle Amministrazioni Pubbliche – Circolare 1/2010/DDI del Ministro per la Pubblica Amministrazione e l'Innovazione
- Informazioni per la gestione delle caselle di Posta Elettronica Certificata – Circolare 2/2010/DDI del Ministro per la Pubblica Amministrazione e l'Innovazione
- Decreto legislativo 26 agosto 2016 n. 179 recante "Modifiche e integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche";

-Circolare AGID 17 marzo 2017, n. 1/2017 G.U. n. 79 del 4/4/2017 -Misure minime di sicurezza ICT per le P.A.

Termini/Acronimi

HW	Hardware
SW	Software
PC	Personal Computer
LAN	Local Area Network: rete trasmissione dati locale
WAN	Wide Area Network: rete trasmissione dati geografica
CED	Centro Elaborazione Dati: struttura preposta alla gestione del Sistema Informativo Comunale
ICT	Information & Communication Technology
DPS	Documento Programmatico sulla Sicurezza
SLA	Service Level Agreement – accordo di servizio, descrive la prestazione richiesta, gli obblighi del fornitore, gli obblighi e i diritti del committente.
SIC	Sistema Informativo Comunale: insieme delle componenti hardware e software.
PEC	Posta Elettronica Certificata

Generalità

La progressiva diffusione delle nuove tecnologie informatiche, e in particolare il libero accesso alla rete Internet dai Personal Computer, espone il ***Comune di Baronissi*** ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, il ***Comune di Baronissi*** ha inteso realizzare il presente Disciplinare all'utilizzo del Sistema Informatico che comprende una serie di indicazioni e modalità operative dirette a evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Tali indicazioni si aggiungono e integrano le specifiche istruzioni fornite a tutti gli incaricati in attuazione del D.lgs. n. 196 del 30.06.2003 "Codice privacy" ed in particolare il relativo allegato B contenente le cosiddette "misure minime" di sicurezza.

Per tutti i casi di dubbia interpretazione e per eventuali chiarimenti tecnici gli utenti del Sistema Informativo del Comune di Baronissi potranno rivolgersi al Servizio Informatico.

1. Utilizzo del Personal Computer

Il Personal Computer (di seguito indicato anche come PC) affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire a innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso al P.C. è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Le password devono essere utilizzate per l'accesso alla rete, a qualsiasi applicazione che lo preveda, per lo screen saver e, quando implementata, per il collegamento a Internet.

Non è consentita l'attivazione della password di accensione (BIOS), senza preventiva autorizzazione da parte del Responsabile del Sistema Informatico.

Il Responsabile del Sistema Informatico per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, anche delegando a terzi con specifico informale mandato, in relazione agli scopi di volta in volta identificati.

Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva verifica del Servizio Informatico che interverrà a seguito di specifica richiesta da parte dell'unità cui è assegnato il PC.

In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente alcuni servizi/uffici, deve essere comunque richiesto parere

preventivo da parte del Responsabile del Servizio Informatico, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti. Sussiste infatti il pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni degli elaboratori e dei sistemi operativi.

Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dal Servizio Informatico dell'Ente (tutela giuridica del software e norme di tutela del diritto d'autore).

All'utente non è consentito modificare le caratteristiche impostate sui PC assegnati, i punti rete di accesso e le configurazioni della rete LAN presente nella sede, salvo autorizzazione del Responsabile del Sistema Informatico.

Il Servizio Informatico verifica il coerente utilizzo delle risorse assegnate al fine di evitarne l'uso improprio o l'accesso a risorse riservate da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.

Il PC deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Lasciare incustodito un elaboratore connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screensaver e la relativa password.

Non è consentita l'installazione sul proprio PC e/o il collegamento sulla rete LAN di nessun dispositivo di memorizzazione, comunicazione o altro (ad esempio pen drive, PC portatili ed altri apparati in genere), se non con l'autorizzazione espressa del Servizio Informatico, previa richiesta da parte dell'ufficio cui è assegnato il PC o il segmento di rete LAN.

Ai sensi del D.lgs. n. 196 del 30.06.2003 è fatto divieto di divulgazione a qualsiasi titolo delle informazioni presenti nelle banche dati dell'Ente se non disciplinate da appositi protocolli di intesa o da specifici obblighi di legge.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Servizio Informatico nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 8) del presente Disciplinare relativa alle procedure di protezione antivirus.

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

2. Utilizzo della rete del Comune di Baronissi

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, potranno essere svolte regolari attività di controllo, amministrazione e backup da parte del Servizio Informatico.

Al fine di garantire la corretta gestione delle politiche di sicurezza delle informazioni è

fatto divieto di replicare su dischi locali dei PC dati, banche dati e documenti sensibili senza esplicita autorizzazione e senza l'adozione di adeguate politiche di sicurezza, quali la cifratura dei dati stessi e l'adozione di politiche di backup comprensive della dotazione di idonei archivi protetti.

Le password d'ingresso alla rete e ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. E' assolutamente proibito accedere alla rete e nei programmi con nomi utente diversi dai propri o dal proprio nel caso di accesso univoco.

Il Responsabile del Sistema Informatico può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati.

E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

E' buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio file di contenuto grafico) su stampanti comuni. In caso di necessità, la stampa in corso può essere cancellata.

Non è consentito l'acquisto di attrezzature informatiche o altri dispositivi da collegare alla rete comunale senza la preventiva verifica del Responsabile del Servizio Informatico per la conformità agli standard tecnici presenti.

3. Utilizzo degli strumenti di telefonia fissa

Gli strumenti di telefonia fissa messi a disposizione dal Comune costituiscono strumento di lavoro e ne è consentito l'utilizzo unicamente per finalità attinenti o comunque connesse all'esercizio dell'attività lavorativa.

E' escluso l'uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza e di necessità. E' in ogni caso è vietato l'uso reiterato e prolungato per fini personali.

Il Responsabile del Servizio, qualora riscontri l'eventualità di un utilizzo improprio di un'utenza telefonica direttamente riferita ad un operatore, al fine di compiere ulteriori verifiche potrà chiedere all'utente interessato i dati relativi a data e ora di inizio delle conversazioni con riferimento al periodo in cui si è verificata l'anomalia. Di tali verifiche è preventivamente informato il soggetto interessato che potrà chiedere di essere ascoltato e di accedere ai relativi documenti. Il Responsabile , qualora ritenga, a seguito delle verifiche compiute, che vi sia stato un utilizzo improprio degli strumenti di telefonia o comunque una violazione delle regole e dei divieti di cui al presente Disciplinare, può segnalare al Dirigente competente di avviare i procedimenti conseguenti.

Il Servizio preposto al controllo, per prevenire o correggere malfunzionamenti del sistema e garantire l'efficienza dello stesso, può consultare i dati relativi al traffico telefonico di ogni settore del Comune e, qualora rilevi un'anomalia, segnalarla al responsabile del settore competente.

4. Gestione delle Password

Le password di ingresso alla rete e di accesso ai programmi sono previste e attribuite dal Servizio Informatico. Al primo accesso sarà necessaria l'autonoma sostituzione da parte degli incaricati.

Le password devono essere lunghe almeno 8 caratteri, (salvo impedimenti tecnici delle applicazioni), formate da lettere (maiuscole e/o minuscole), numeri e caratteri speciali quali & % ^ # $, ricordando che lettere maiuscole e minuscole hanno significati diversi per i sistemi, evitando ovviamente contenuti di senso logico immediato che sono facilmente individuabili (per es. nomi/date di nascita e simili).

La password deve essere immediatamente sostituita, dandone comunicazione al Responsabile del Servizio Informatico, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Servizio Informatico.

E' dato comunicare tempestivamente eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, sia all'Ufficio Personale che ai servizi informatici al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione/blocco delle password ove necessario.

5. Utilizzo di Personal Computer portatili

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, trasferte lavorative, altro), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Eventuali configurazioni di tipo accesso remoto, dirette verso la rete comunale o attraverso Internet, devono essere autorizzate esclusivamente a cura del Servizio Informatico. E' vietato utilizzare le suddette connessioni all'interno delle sedi comunali se contemporaneamente connessi alla rete LAN.

6. Uso della posta elettronica

La casella di posta elettronica istituzionale, assegnata all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Si rammenta che i sistemi di posta elettronica non consentono al momento di garantire la riservatezza delle informazioni trasmesse, si raccomandano gli utenti di non inoltrare dati e informazioni classificabili "sensibili" o "personali" con questo mezzo.

E' fatto divieto di utilizzare le caselle di posta elettronica del tipo nomeutente@comune.baronissi.sa.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list non attinenti la propria attività o funzione svolta per l'Ente, salvo diversa ed esplicita autorizzazione.

E' buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. E' previsto un dimensionamento massimo per ciascuna casella in relazione alla disponibilità di spazio dei sistemi di posta di volta in volta disponibili, che non potrà essere superato per evitare l'appesantimento della gestione dei server stessi.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Comune di Baronissi ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata o autorizzata dal Responsabile cui si riferisce l'attività. In ogni modo, è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria (Gestione Protocollo).

E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per le comunicazioni ufficiali è obbligatorio avvalersi di altri strumenti quali la **Posta Elettronica Certificata del Protocollo**.

Si rammenta che il valore legale delle comunicazioni inviate tramite Posta Elettronica Certificata (PEC) equivale a quello di un invio effettuato tramite raccomandata A/R. Gli assegnatari di caselle PEC sono tenuti a consultare con frequenza almeno giornaliera le proprie caselle PEC e a gestire con la necessaria cura la relativa corrispondenza, facendo riferimento alle procedure per la gestione della corrispondenza (Gestione Protocollo).

Per la trasmissione di file all'interno del Comune è obbligatorio utilizzare il file server OwnCloud e non altri strumenti.

E' obbligatorio controllare con il Software antivirus i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o ftp non conosciuti).

E' vietato inviare catene telematiche. Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Servizio Informatico. Non si devono in alcun caso attivare gli allegati di tali messaggi.

7. Uso della rete Internet e dei relativi servizi

Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. E' proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.

E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile del Servizio Informatico.

E' vietato ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.

E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

E' vietata la partecipazione a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nickname), se non attinenti l'attività lavorativa svolta.

Il Responsabile del Servizio Informatico potrà decidere di applicare, per singoli e gruppi di utenti, politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con l'Amministrazione e con i Responsabili dei Settori, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.

8. Protezione antivirus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico comunale mediante virus o mediante ogni altro software aggressivo.

Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.

Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al Servizio Informatico.

Non è consentito l'utilizzo di dispositivi USB di dubbia provenienza e/o non controllato.

9. Osservanza delle disposizioni in materia di Privacy

E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza.

10. Inosservanza della normativa

Il mancato rispetto delle regole contenute nel presente Disciplinare potrebbe causare danni e malfunzionamenti del Servizio Informatico Comunale esponendo di conseguenza il dipendente al rischio di provvedimenti disciplinari nonché alle azioni civili e penali previste dalla normativa vigente.

11. Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Disciplinare.

Il presente Disciplinare è comunque soggetto a revisione con frequenza annuale.

Allegato A

Codice in materia di protezione dei dati personali

(Decreto legislativo 30 giugno 2003, n. 196)

Definizioni (art. 4)

Ai fini del presente codice si intende per:

a) **"trattamento",** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) **"dato personale",** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) **"dati identificativi",** i dati personali che permettono l'identificazione diretta dell'interessato;

d) **"dati sensibili",** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) **"dati giudiziari",** i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) **"titolare",** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) **"responsabile",** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) **"incaricati",** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) **"interessato",** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) **"comunicazione",** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro

messa a disposizione o consultazione;

m) **"diffusione"**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) **"dato anonimo",** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) **"blocco",** la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) **"banca di dati",** qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) **"Garante",** l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.