COMUNE DI ANCONA

DETERMINAZIONE DEL DIRIGENTE

del 22/12/2009 N. 3001

SERVIZIO SISTEMI INFORMATIVI

Oggetto : Atto non comportante impegno di spesa.
ADOZIONE MISURE ATTUATIVE SUGLI AMMINISTRATORI DI SISTEMA AI SENSI DEL PROVVEDIMENTO DEL GARANTE DELLA PRIVACY DEL 27 NOVEMBRE 2008

Servizio Finanziario

Visto, si attesta che non occorre impegno di spesa.

……

……

Ancona 22/12/2009

Il Responsabile U.O. Interventi

Il Responsabile Servizio Finanziario
DOTT.SSA SERI DONATELLA

Destinatari :

- **Assessore**
- **Direttore Area**
- **Segreteria** (originale)
- **SERVIZIO SISTEMI INFORMATIVI**

(SERVIZIO SISTEMI INFORMATIVI)

- **SERVIZIO ORGANIZZAZIONE E PERSONALE**

Ancona, 21/12/2009

Il Dirigente del Servizio
DOTT. BATTISTINI GIOVANNA - 11102

IL DIRIGENTE DEL SETTORE
INFORMATICA E INNOVAZIONE
Ing. Giovanna Battistini

VISTI:

- il decreto legislativo 30 giugno 2003, n. 196 nel quale sono raccolte tutte le disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali ed alle attività connesse;
- il Documento Programmatico per la Sicurezza, redatto ai sensi del D.Leg.vo n. 196/2003, adottato dal Comune di Ancona con Deliberazione di Giunta n. 828 del 30.12.2005, e successive modifiche e integrazioni
- il Provvedimento del Garante per la Protezione dei dati personali del 27/11/2008 relativo a: "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come integrato e modificato dal Provvedimento del 25/6/2009;

PRESO ATTO che con Decreto del Sindaco n. 192 del 15/12/2009 di designazione quale responsabile del trattamento dei dati personali, è stato dato mandato al Dirigente del Settore Informatica e Innovazione di individuare le misure attuative del Provvedimento succitato;

PRESO ATTO che con delibera n. 326 del 15/12/2009 è stato aggiornato il Documento Programmatico sulla Sicurezza del Comune di Ancona prevedendo all'art. 6 , tra i compiti di natura amministrativa del Dirigente del Settore Informatica e Innovazione, la predisposizione di un apposito documento che contenga le "Misure attuative sugli Amministratori di Sistema" e di procedere alla loro nomina ai sensi dei provvedimenti del Garante per la protezione dei dati personali del 27.11.2008 e 25.06.2009;

CONSTATATA l'esigenza di valutare con particolare attenzione l'attribuzione delle funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema in quanto equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza, e amministratori di sistemi software complessi, laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali;

VALUTATO quindi che risulta necessario, per l'attuazione del Provvedimento, la preventiva individuazione delle tipologie degli amministratori di sistema e dei profili di autorizzazione ;

VISTO il documento "Misure attuative del provvedimento sugli Amministratori di Sistema" redatto dal Settore Informatica e Innovazione contenente:

- definizione ruoli, compiti e responsabilità, profilo di autorizzazione degli amministratori di sistema
- requisiti , modalità di nomina, revoca e formazione degli amministratori di sistema
- disposizione delle misure di carattere organizzativo che stabiliscano le procedure operative e favoriscano una più agevole conoscenza dell'esistenza di determinati ruoli tecnici
- previsione degli aspetti tecnici del provvedimento (in particolare, la conservazione dei log degli accessi effettuati dagli amministratori di sistema)
- modulistica relativa alla nomina, le linee guida e le note operative;

RITENUTO di procedere con successivo atto alla nomina individuale degli Amministratori di sistema con l'elenco delle funzioni ad essi attribuite, dopo la valutazione delle caratteristiche soggettive;

DATO ATTO che il presente provvedimento non comporta per sua natura impegno di spesa;

DETERMINA

I. Di approvare, per le motivazioni espresse in premessa, il documento " Misure attuative sugli Amministratori di Sistema ai sensi del Provvedimento della Privacy del 27 novembre 2008" conservato agli atti del Settore;

II. Di pubblicare nel sito Internet e nell' apposita sezione, dedicata alla Privacy, della Intranet interna dell'Amministrazione comunale il documento suddetto;

III. Di dare atto che il presente provvedimento non comporta per sua natura impegno di spesa;

VI. Di dare esecuzione al procedimento con la presente disposto designandone, a norma dell'art. 5 della legge 241/1990, a responsabile la sottoscritta

DOCUMENTAZIONE DI RIFERIMENTO CONSERVATA AGLI ATTI DELL'UFFICIO - MISURE ATTUATIVE SUGLI AMMINISTRATORI DI SISTEMA ai sensi del Provvedimento del Garante della Privacy del 27/11/2008
DOCUMENTAZIONE TRASMESSA ALLA RAGIONERIA :

Dirigente Settore
Informatica e Innovazione
Ing. Giovanna Battistini

Il Responsabile del Procedimento
Ing Giovanna Battistini

Servizio Finanziario

IL PRESENTE ATTO NON VA PUBBLICATO NEL SITO WEB, IN QUANTO NON RIENTRA NELLE IPOTESI PREVISTE DALL'ART. 31 DELLA DELIBERA DI G.M. N. 48 DEL 19/02/2008

Il Dirigente del Servizio

_____

OPPURE

IL PRESENTE ATTO VA PUBBLICATO NEL SITO WEB, AI SENSI DELL'ART. 31 DELLA DELIBERA DI G.M. N. 48 DEL 19/02/2008, ALLA SEZIONE:

☐ **INCARICHI PER CONSULENZE – STUDI - RICERCHE**

☐ **INCARICHI PER COLLABORAZIONI**

☐ **INCARICHI PER PRESTAZIONI DI SERVIZI**

☐ **INCARICHI PER SERVIZI INGEGNERIA - ARCHITETTURA**

☐ **INCARICHI PER PATROCINII LEGALI – RAPPRESENTANZE IN GIUDIZIO, ASSISTENZA E DOMICILIAZIONE**

(BARRARE LA CASELLA CORRISPONDENTE)

☐ **IN FORMA INTEGRALE**

☐ **IN FORMA PARZIALE** [1] **(COME DA COPIA TRASMESSA ALL'UFFICIO DETERMINAZIONI)**

(BARRARE LA CASELLA CORRISPONDENTE)

Il Dirigente del Servizio

_____

(1) VANNO STRALCIATE LE PARTI CHE RIGUARDANO IL RISPETTO DEL D.Lgs. 196/2003 SULLA PRIVACY E QUELLE CHE NON RIENTRANO IN UNA DELLA FATTISPECIE DI CUI ALLE SEZIONI INDICATE

COMUNE DI ANCONA
Settore Informatica e innovazione

Misure attuative sugli Amministratori di Sistema

ai sensi del Provvedimento del Garante della Privacy del 27/11/2008

Codice Versione: DEF-1

Approvazione: Determina Dirigenziale n. 3001 del 22/12/2009

Distribuzione: Aree/settori/servizi dell'Ente

COMUNE DI ANCONA
Settore Informatica e innovazione

INDICE GENERALE

DEFINIZIONI

Account:	insieme di funzionalità, strumenti e contenuti attribuiti ad un utente in un determinato contesto operativo. Attraverso l'account, il sistema informatico od anche il software applicativo, rende disponibili agli utenti contenuti e funzionalità personalizzati rispetto al proprio profilo di autorizzazione.
AdS:	Amministratore di Sistema.
Agent:	programma o componente software capace di risolvere delle problematiche interagendo con altri software.
Audit:	in ambito sicurezza informatica, è la valutazione tecnica manuale o sistematica misurabile di un sistema o di un'applicazione.
Backdoor:	(letteralmente porta sul retro) è un mezzo di accesso ad un sistema che aggira i meccanismi di sicurezza.
Backup:	(copia di sicurezza) operazione periodica di duplicazione su differenti supporti di memoria dei dati o dei programmi presenti sui dischi di personal computer o di server.
Domain Administrator:	(amm. di dominio) tipologia di amministratore di sistema con elevati livelli di autorizzazione (v. Allegato A). In caso di singolo dominio è equivalente all'Enterprise Administrator.
DPsS:	(o DPS) Documento Programmatico sulla Sicurezza è un obbligo previsto dal D.Lgs. 196/2003; contiene la fotografia dello stato della sicurezza dell'Ente, l'analisi del rischio e le contromisure a tutela delle informazioni gestite.
Dump:	modalità di backup dei database (DBMS) tramite la creazione di un file contenente dichiarazioni SQL per la definizione dello schema e per l'inserimento dei dati contenuti.
Elenco AdS:	documento obbligatorio previsto al punto 4.3 del Provvedimento del Garante della Privacy del 27 novembre 2008.
Enterprise Administrator:	Amministratore di Sistema al massimo livello di autorizzazione (v. Allegato A).
Export:	operazione di esportazione di dati o configurazioni da servizi o applicativi software.
Log:	registro cronologico degli eventi.
Logbook:	documento di registrazione di tutti gli eventi.
Log di Accesso:	(o Access Log) registrazione cronologica delle operazioni di accesso su singolo sistema / rete / dominio.
Log di Sistema:	(o System Log) registrazione cronologica degli eventi significativi verificatisi in un singolo sistema.
Profilo di autorizzazione:	insieme di informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
Resp. del trattamento:	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali (D.Lgs. 196/03).

Resp. Esterno del tratt.:	figura non esplicitamente prevista nel Codice Privacy, ma derivante dall'interpretazione dottrinale degli articoli 4 comma 1 punto g e 29 del D.Lgs 196/03. La nomina risulta necessaria (anche se non vi sono estremi di obbligatorietà), ogni qualvolta il Titolare decida di affidare all'esterno dell'Ente un trattamento.
Roll-back:	(lett. Rotolare indietro) annullamento delle ultime operazioni effettuate senza modifiche ai dati o alla configurazione.
Share di Rete:	spazio di condivisione dei dati in rete.
Snapshot:	(lett. istantanea) salvataggio di una macchina (configurazione, applicativi e dati) ad un dato istante.
Titolare del Trattamento:	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 (D.Lgs. 196/03).
Troubleshooting:	(lett. eliminazione del problema) processo di ricerca logica e sistematica delle cause di un problema.

INTRODUZIONE

Il legislatore italiano ha promulgato negli ultimi anni una serie di norme riguardanti il tema della sicurezza delle informazioni.

Sono immediatamente individuabili due filoni principali, il primo a tutela ".. dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.." ed il secondo a garanzia del buon funzionamento e protezione dei sistemi informatici (D.Lgs. 518/92 e Legge n. 547/1993).
La normativa di riferimento per il primo filone è il Testo Unico sulla privacy, emanato con D.Lgs. 196/03, che abroga tutte le precedenti norme, come la Legge n. 675/1996 ed il D.P.R. n. 318/1999. Queste due ultime norme definivano una figura di Amministratore delle password, che nulla aveva a che vedere con le mansioni di un attuale *Domain Administrator*: L'iter legislativo aveva stravolto l'idea iniziale di affidare solo ai sistemi informatici la conservazione delle credenziali di autenticazione, obbligando paradossalmente gli operatori coinvolti ad effettuare operazioni da considerare, nella migliore delle ipotesi, incidenti della sicurezza, o peggio, reati penali.

Con l'introduzione del D.Lgs. 196/03 la figura di amministratore delle password scompare e si trasferiscono sul Titolare del trattamento le responsabilità organizzative e tecniche.
Questa concentrazione formale di responsabilità sul Titolare del trattamento, non risolve in ogni caso il problema degli accessi, incontrollati ed incontrollabili, a tutti i dati personali e sensibili presenti nella rete aziendale, da parte degli Amministratori di Sistema.

Il Garante della Privacy, consapevole della rilevanza e della delicatezza dei trattamenti di dati personali effettuati da coloro che svolgono mansioni di Amministratori di Sistema, ha emanato nell'ultimo provvedimento del 27 novembre 2008 (Allegato D – Bibliografia e Sitografia), una serie di prescrizioni volte a tutelare la riservatezza delle informazioni conservate nella rete aziendale, lasciando al singolo Titolare del trattamento la scelta delle modalità di applicazione più specifiche.

Il presente documento ha l'obiettivo di definire esattamente ruolo, compiti e responsabilità delle figure c.d. Amministratori di sistema, coinvolte in prima linea nella tutela della riservatezza, integrità e disponibilità delle informazioni.

MISURE ATTUATIVE

ART. 1 – DEFINIZIONE DI AMMINISTRATORE DI SISTEMA, COMPITI E RESPONSABILITA'

a) In ambito informatico, l'Amministratore di Sistema è la figura professionale che si occupa della gestione e della manutenzione di un sistema di elaborazione e delle sue componenti.

b) I principali compiti di un Amministratore di Sistema sono i seguenti:

- Monitorare l'infrastruttura informatica di competenza attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
- Introdurre ed integrare nuove tecnologie negli ambienti esistenti;
- Installare e configurare nuovo hardware/software sia lato client sia lato server;
- Applicare le patch e gli aggiornamenti necessari al software di base ed applicativo, modificare le configurazioni in base alle esigenze dell'Ente;
- Gestire e tenere aggiornati gli account utente ed i relativi profili di autorizzazione;
- Fornire risposte alle questioni tecniche sollevate dall'utenza, porre rimedio ai problemi/guasti tramite tecniche di *troubleshooting*;
- Pianificare e verificare la corretta esecuzione dei backup e delle repliche;
- Documentare le operazioni effettuate (*Logbook*), le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni ai problemi;
- Ottenere le migliori prestazioni possibili con l'hardware a disposizione;
- Operare secondo le prescrizioni di sicurezza e le procedure interne previste.

c) Nell'ambito dell'Ente è possibile individuare tipologie specifiche di Amministratore di Sistema, differenziate per livello di autorizzazione e profilo (v. *Allegato A*).

d) Si possono individuare Amministratori di Sistema interni o esterni all'Ente; la nomina può essere diretta se viene fatta dal Dirigente del Settore Informatica e Innovazione o indiretta se viene fatta dal responsabile esterno del trattamento, opportunamente nominato secondo quanto previsto dal Documento Programmatico della Sicurezza (DPsS).

ART. 2 – REQUISITI DI NOMINA

L'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

ART. 3 –MODALITA' DI NOMINA DIRETTA

Il Dirigente del Settore Informatica e innovazione, in qualità di Amministratore del Sistema Informatico Comunale, nomina gli Amministratori di Sistema ai sensi dell'art. 2 del presente documento.

La nomina deve essere individuale, per iscritto e deve riportare, come da *Allegato B*:

- cognome e nome, codice fiscale, data e luogo di nascita, dell'Amministratore di Sistema nominato;
- le tipologie di Amministratore di Sistema ed il profilo di autorizzazione che si intende affidare alla persona fisica, come da *Allegato A*;
- l'ambito analitico di autorizzazione.

ART. 4 – MODALITA' DI NOMINA INDIRETTA

Il responsabile esterno del trattamento nomina gli Amministratori di Sistema esterni ai sensi dell'art. 2 del presente documento ed è tenuto ad inviare al Dirigente del Settore Informatica e Innovazione i seguenti documenti:

- dichiarazione circa il possesso dei requisiti di cui all'Art. 2 da parte dei nominati;
- copia della nomina della persona fisica ad Amministratore di Sistema;
- dichiarazione circa la redazione ed aggiornamento del proprio DPsS;
- dichiarazione sull'adempimento dell'obbligo di formazione degli Amministratori nominati, secondo quanto previsto dalla normativa privacy.

Il Dirigente del Settore Informatica e Innovazione integra l'Elenco degli Amministratori di Sistema con l'inserimento dei nuovi amministratori esterni nominati.

ART. 5 – REVOCA DELLA NOMINA

a) Il Dirigente del Settore Informatica e Innovazione può revocare l'incarico di Amministratore di Sistema in caso di:

   - inadempienza o inosservanza delle prescrizioni di sicurezza;
   - violazione di quanto previsto dal presente documento;
   - sopravvenuta mancanza dei requisiti ai sensi dell'Art. 2;
   - modifica del rapporto contrattuale di lavoro dell'Amministratore di Sistema.

b) La revoca degli Amministratori di Sistema legati contrattualmente a fornitori esterni all'Ente è compito del Responsabile Esterno del trattamento, che, direttamente o su richiesta del Dirigente del Settore Informatica e innovazione, provvede ad effettuare la comunicazione di revoca all'Amministratore di Sistema.

c) In considerazione dei risvolti tecnici ma soprattutto di continuità ed affidabilità dei servizi, la revoca dell'incarico di un Amministratore di Sistema dovrà seguire la procedura indicata all'Art. 6.

ART. 6 – PROCEDURA DI REVOCA DEGLI AMMINISTRATORI DI SISTEMA

La revoca dell'incarico di un Amministratore di Sistema prevede le seguenti azioni da eseguire rigorosamente nell'ordine specificato:

- Verificare l'esistenza di eventuali servizi lanciati (erroneamente) con l'*account* dell'Amministratore di Sistema; assegnare al servizio un *account* specifico per l'esecuzione della tipologia di servizi interessata;

- Controllare l'esistenza di eventuali *backdoor* (*account* o applicative, accessi remoti, autorizzate o non autorizzate) riferibili all'Amministratore di Sistema da disabilitare;
- Nel caso non sia già esistente, creare un *account* amministrativo con lo stesso profilo di autorizzazione dell'Amministratore di Sistema da disabilitare, da assegnare al nuovo Amministratore di Sistema (sostituto);
- Disabilitare l'*account* dell'Amministratore di Sistema revocato;
- Verificare che tutti i servizi collegati al profilo di autorizzazione dell'Amministratore di Sistema risultino perfettamente funzionanti;
- Comunicare la disabilitazione dell'account di Amministratore di Sistema e la revoca dell'incarico alla persona fisica.

ART. 7 – FORMAZIONE ED AGGIORNAMENTO ANNUALE

Al fine di migliorare il livello di sicurezza dell'Ente, il Dirigente del Settore Informatica e Innovazione organizza con cadenza annuale, sessioni di formazione ed aggiornamento sui temi della sicurezza nel trattamento dei dati e su temi specifici connessi ai compiti di amministrazione di sistema.

ART. 8 – REDAZIONE E AGGIORNAMENTO DOCUMENTAZIONE

Gli estremi identificativi delle persone fisiche nominate Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un "Elenco degli Amministratori di Sistema" redatto, aggiornato e trasmesso all'Ufficio Coordinamento Privacy a cura del Dirigente del Settore Informatica e Innovazione, secondo quanto previsto dal Documento Programmatico sulla Sicurezza del Comune di Ancona.

ART. 9 – VERIFICA DELLE ATTIVITA' DEGLI AMMINISTRATORI DI SISTEMA

a) Il Dirigente del Settore Informatica e Innovazione verifica periodicamente, e con cadenza annuale, l'attività degli Amministratori di Sistema attraverso audit interni, al fine di accertarne la conformità alle mansioni attribuite e la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti.

b) Il Dirigente del Settore Informatica e Innovazione si riserva di comunicare al Titolare del trattamento, qualsiasi comportamento non conforme al presente documento per gli opportuni provvedimenti del caso.

ART. 10 – REGISTRAZIONE DEGLI ACCESSI E DEGLI EVENTI

a) Il Dirigente del Settore Informatica e Innovazione adotta sistemi idonei per garantire la registrazione degli accessi logici (autenticazione informatica) da parte degli Amministratori di Sistema.

b) Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

c) I sistemi ed i dispositivi infrastrutturali ritenuti vitali e critici (per sensibilità dei dati contenuti o in quanto connessi direttamente alla continuità di servizi) dovranno prevedere anche la

registrazione degli eventi (*system log*). Per un miglior controllo e governo dell'infrastruttura informatica dell'Ente, sarà opportuno estendere la registrazione a tutti gli eventi di tutti i dispositivi collegati.

ART. 11 – ESPORTAZIONE E CONSERVAZIONE DEGLI ACCESS LOG

a) Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a 6 mesi. Gli access log possono essere cancellati solamente alla scadenza dei 6 mesi.

b) La conservazione degli access log può essere on site o in outsourcing. In ogni caso dovrà essere in linea con le regole tecniche contenute nella deliberazione CNIPA n. 11/2004 e successive modificazioni.

c) Le modalità di registrazione, esportazione e conservazione dei log saranno dettagliate con apposita procedura operativa.

ART. 12 – SALA MACCHINE

a) La Sala Macchina è considerata "Zona di massima sicurezza" e accessibile solamente agli Amministratori di Sistema individuati dal Dirigente del Settore Informatica e Innovazione. L'accesso al personale non autorizzato è vietato.

b) E' chiusa a chiave e protetta da adeguati sistemi di sicurezza fisica.

c) Ogni singolo accesso del personale alla sala macchine deve essere registrato. Eventuali tecnici esterni devono essere identificati, autorizzati e registrati. In ogni caso il personale esterno può accedere solamente sotto stretta sorveglianza di un Amministratore di Sistema autorizzato.

ART. 13 – LIBRO DI BORDO SALA MACCHINE – LOGBOOK

a) E' istituito il "Libro di bordo Sala Macchine" o "*Logbook* Sala Macchine" dove sono riportati tutti gli eventi sensibili alla riservatezza, integrità e disponibilità delle informazioni.

b) Nel "*Logbook* Sala Macchine" devono essere riportati tutti gli eventi, come:

- Registrazione accessi sala macchine di personale interno ed esterno;
- Installazioni/Disinstallazioni/Modifica delle configurazioni hardware o software;
- Lavori di riparazione e di manutenzione;
- Riavvii attesi, crash inattesi, interruzioni di servizio o di alimentazione;
- Problemi agli impianti di comunicazione, alimentazione, protezione, antincendio e climatizzazione;
- Attivazione degli allarmi (intrusione, temperatura, allagamento).

c) Ogni registrazione deve prevedere:

a) Progressivo evento;
b) Data/Ora evento, inizio attività o ingresso;
c) Data/Ora chiusura evento, fine attività o uscita;
d) Sistemi e dispositivi coinvolti;

e) Tipologia intervento (software / hardware / networking);
f) Operazione effettuata;
g) *Roll-back* possibile (si/no);
h) Possibile impatto dell'evento/operazione (Basso / Medio / Alto);
i) Eventuali problemi riscontrati;
j) Livello Emergenza (min = 0; MAX = 5);
k) Eventuale azione correttiva, strategia di risoluzione;
l) Tecnico/Responsabile di riferimento;
m) Operatori, tecnici intervenuti e Firma del compilatore;
n) Eventuali Note.

ART. 14 – DIVIETI E DISPOSIZIONI

a) La Documentazione Interna dei Settore Informatica e Innovazione, in particolare la documentazione relativa all'infrastruttura di rete, alla configurazione dei sistemi o degli applicativi, alle impostazioni o abilitazioni degli utenti, deve essere conservata in luogo sicuro, preferibilmente non accessibile in rete. L'accesso a detta documentazione è consentito solamente al personale nominato Amministratore di Sistema, per il solo tempo necessario alla consultazione e all'aggiornamento.

b) E' vietato trasportare la Documentazione Interna del Settore Informatica in qualsiasi formato o media all'esterno dell'Ente. Il divieto include l'invio di mail/fax/lettere contenenti documentazione anche parziale, la compilazione o la risposta ad interviste/indagini di mercato effettuate tramite telefono/fax/lettera.

c) Gli *account* e le relative password di livello Amministratore di Sistema non devono essere rivelate a nessuno per nessun motivo. E' vietato trasmettere in qualsiasi formato anche criptato dette informazioni.

d) In caso di perdita di segretezza di una password di livello Amministratore di Sistema, è necessario comunicare l'evento al Dirigente del Settore Informatica e innovazione, effettuarne immediatamente la modifica e verificare che non siano stati creati nel frattempo nuovi utenti o modificati profili di autorizzazione.

e) In *Allegato C* sono riportate le "Linee guida e note operative" specifiche per gli Amministratori di Sistema interni ed esterni.

2. ALLEGATO A – TIPOLOGIA DI AMMINISTRATORE E PROFILI DI AUTORIZZAZIONE

Sono individuate le seguenti tipologie ed il relativo profilo di autorizzazione:

Tipologia	Livello Sicurezza	Ruolo	Profilo di autorizzazione
Enterprise Administrator 	MAX	Livello più alto di autorizzazione nell'ambito della rete dell'Ente. Nel caso di singolo dominio le figure di Enterprise Administrator e Domain Administrator coincidono.	Autorizzato: 1. all'accesso completo a tutti i dati e a tutte le macchine appartenenti a tutti i domini della rete (a meno di diversa ed esplicita configurazione); 2. alla creazione degli *account* ed abilitazione degli accessi agli Administrator di livello 0, 1 e 2 di tutti i domini; 3. all'analisi e controllo dei log di tutte le macchine appartenenti a tutti i domini e dei dispositivi di tutta la rete (a meno di diversa ed esplicita configurazione).
Domain Administrator 	0	Livello più alto di autorizzazione nell'ambito del singolo Dominio della rete dell'Ente. Nel caso di singolo dominio le figure di Enterprise Administrator e Domain Administrator coincidono.	Autorizzato: 1. all'accesso completo a tutti i dati ed a tutte le macchine appartenenti ad un singolo dominio della rete (a meno di diversa ed esplicita configurazione); 2. alla creazione degli *account* e all'abilitazione degli accessi agli Administrator di livello 0, 1 e 2 del solo dominio di appartenenza; 3. all'analisi e controllo dei log di tutte le macchine appartenenti al solo dominio di appartenenza e dei dispositivi della porzione di rete gestita (a meno di diversa ed esplicita configurazione).

Server Administrator 	1	Amministratore di un singolo sistema server.	Autorizzato: 1. all'accesso completo al sistema ed ai dati contenuti nel server (a meno di diversa ed esplicita configurazione; es. escluso db); 2. a compiere qualsiasi operazione sistemistica e di modifica della configurazione del server; 3. all'analisi e controllo dei log.
Account Administrator 	1	Amministratore degli *account* utente per il solo dominio di appartenenza.	Autorizzato: 1. alla creazione/disabilitazione degli *account utente*; 2. all'assegnazione del profilo di autorizzazione all'*account utente*.
Network Administrator 	1	Amministratore dell'infrastruttura di rete e di comunicazione	Autorizzato: 1. all'accesso completo ai dispositivi e linee di comunicazione dati; 2. a compiere qualsiasi operazione di modifica della configurazione dei dispositivi di comunicazione dati; 3. all'analisi e controllo dei log e del traffico dati.
Security Administrator 	1	Amministratore dei dispositivi di sicurezza	Autorizzato: 1. all'accesso completo ai dispositivi di sicurezza (es. Firewall, Antivirus, Log Management, Traffic analyzer); 2. a compiere qualsiasi operazione di modifica della configurazione dei dispositivi di sicurezza; 3. all'analisi e controllo dei log.
Data Base Administrator 	1	Amministratore di un database server o di una singola istanza di database	Autorizzato: 1. all'accesso completo al motore del database ed ai dati memorizzati; in casi particolari è possibile autorizzare anche la singola istanza di database; 2. a compiere qualsiasi operazione di modifica della configurazione e degli schemi dei database; 3. all'analisi e controllo dei log.

Backup Administrator 	1	Amministratore dei backup e delle repliche dei dati	Autorizzato all'accesso (almeno in lettura): 1. dei dump dei database (o direttamente delle istanze in caso di utilizzo di *agent*); 2. delle *share* di rete; 3. dei *system state* e degli *snapshot* delle macchine; 4. delle configurazioni (che necessitano di backup); 5. degli *export* di specifici servizi; 6. dei log di tutte le macchine della rete.
Service / Application Administrator 	2	Amministratore di un singolo servizio o applicazione (es. mail server, web server, application server)	Autorizzato: 1. alla gestione, modifica delle configurazione, stop/start del singolo servizio o applicazione; 2. all'analisi e controllo dei log specifici del servizio o applicazione.
Local Administrator - Technical support 	2	Amministratore locale di singoli sistemi *client*	Autorizzato: 1. all'accesso completo ad un insieme specificato nella nomina di sistemi *client* ed ai dati contenuti nei dispositivi di memorizzazione (a meno di diversa ed esplicita configurazione); 2. all'analisi e controllo dei log locali.

3. ALLEGATO B – MODULISTICA

NOMINA AD AMMINISTRATORE DI SISTEMA

In conformità alla normativa vigente ed in particolare al provvedimento del Garante della Privacy del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), così come modificato con Provvedimento del 25/6/2009, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema", il Dirigente del Settore Informatica e Innovazione nomina

Amministratore di Sistema

Cognome e nome: _____

Codice fiscale: _____

Data e luogo di nascita: _____ _____

Tipologia Amministratore	Profilo di autorizzazione
☐ Enterprise Administrator	Autorizzato: 1. all'accesso completo a tutti i dati e a tutte le macchine appartenenti a tutti i domini della rete (a meno di diversa ed esplicita configurazione); 2. alla creazione degli *account* ed abilitazione degli accessi agli Administrator di livello 0, 1 e 2 di tutti i domini; 3. all'analisi e controllo dei log di tutte le macchine appartenenti a tutti i domini e dei dispositivi di tutta la rete (a meno di diversa ed esplicita configurazione).
☐ Domain Administrator	Autorizzato: 1. all'accesso completo a tutti i dati ed a tutte le macchine appartenenti ad un singolo dominio della rete (a meno di diversa ed esplicita configurazione); 2. alla creazione degli *account* e all'abilitazione degli accessi agli Administrator di livello 0, 1 e 2 del solo dominio di appartenenza; 3. all'analisi e controllo dei log di tutte le macchine appartenenti al solo dominio di appartenenza e dei dispositivi della porzione di rete gestita (a meno di diversa ed esplicita configurazione).
☐ Server Administrator	Autorizzato: 1. all'accesso completo al sistema ed ai dati contenuti nel server (a meno di diversa ed esplicita configurazione; es. escluso db); 2. a compiere qualsiasi operazione sistemistica e di modifica della configurazione del server; 3. all'analisi e controllo dei log.
☐ Account Administrator	Autorizzato: 1. alla creazione/disabilitazione degli *account utente*;

	2. all'assegnazione del profilo di autorizzazione all'*account utente*.
☐ Network Administrator	Autorizzato: 1. all'accesso completo ai dispositivi e linee di comunicazione dati; 2. a compiere qualsiasi operazione di modifica della configurazione dei dispositivi di comunicazione dati; 3. all'analisi e controllo dei log e del traffico dati.
☐ Security Administrator	Autorizzato: 1. all'accesso completo ai dispositivi di sicurezza (es. Firewall, Antivirus, Log Management, Traffic analyzer); 2. a compiere qualsiasi operazione di modifica della configurazione dei dispositivi di sicurezza; 3. all'analisi e controllo dei log.
☐ Data Base Administrator	Autorizzato: 1. all'accesso completo al motore del database ed ai dati memorizzati; in casi particolari è possibile autorizzare anche la singola istanza di database; 2. a compiere qualsiasi operazione di modifica della configurazione e degli schemi dei database; 3. all'analisi e controllo dei log.
☐ Backup Administrator	Autorizzato all'accesso (almeno in lettura): 1. dei dump dei database (o direttamente delle istanze in caso di utilizzo di *agent*); 2. delle *share* di rete; 3. dei *system state* e degli *snapshot* delle macchine; 4. delle configurazioni (che necessitano di backup); 5. degli *export* di specifici servizi; 6. dei log di tutte le macchine della rete.
☐ Service/Application Administrator	Autorizzato: 1. alla gestione, modifica delle configurazione, stop/start del singolo servizio o applicazione; 2. all'analisi e controllo dei log specifici del servizio o applicazione.
☐ Local Administrator - Technical support	Autorizzato: 1. all'accesso completo ad un insieme specificato nella nomina di sistemi *client* ed ai dati contenuti nei dispositivi di memorizzazione (a meno di diversa ed esplicita configurazione); 2. all'analisi e controllo dei log locali.

Ambito analitico di autorizzazione:

Tipologia Amministratore	Sistema in cui riveste il profilo di amministratore

che pertanto dichiara:

a) di possedere le caratteristiche di esperienza, capacità ed affidabilità necessarie alla funzione attribuita;
b) di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
c) di aver preso visione del "Regolamento per l'accesso e l'uso della rete informatica e telematica del Comune di Ancona" e delle "Misure Attuative del Provvedimento sugli Amministratori di Sistema", in particolare dell'*Allegato C*;

dichiara inoltre che sarà sua cura:

d) informare prontamente il Dirigente del Settore Informatica e innovazione di tutte le questioni rilevanti ai fini di legge ed in termini di sicurezza;
e) non comunicare e non diffondere i dati personali conosciuti o ai quali si abbia avuto accesso nello svolgimento delle prestazioni contrattuali, se non autorizzati dal Titolare del Trattamento;
f) non comunicare a nessuno le eventuali informazione acquisite durante la permanenza negli uffici comunali;
g) non utilizzare i dati trattati e le informazioni acquisite per finalità che non siano strettamente inerenti all'oggetto del contratto o della convenzione o dell'accordo, che condiziona la presente autorizzazione;
h) osservare la massima riservatezza in merito alle informazioni ottenute nello svolgimento dell'attività professionale, incluse le informazioni relative alla situazione di sicurezza dell'Ente, come sistemi operativi, applicativi software, documentazione, architettura e connessioni di rete;
i) attenersi, in ogni caso, a tutte le istruzioni che saranno impartite dal Dirigente del Settore Informatica e innovazione.

La presente autorizzazione è condizionata, per oggetto e durata, al contratto in corso di esecuzione tra le parti e si intenderà revocata di diritto alla scadenza del rapporto o alla risoluzione, per qualsiasi causa, dello stesso.

Ancona, li _____ Per accettazione di tutte le condizioni

Il Dirigente Settore Informatica e Innovazione L'Amministratore di Sistema

_____ _____

4. ALLEGATO C – LINEE GUIDA E NOTE OPERATIVE PER GLI AMMINISTRATORI INTERNI ED ESTERNI

a) Attenersi scrupolosamente a tutte le procedure operative e segnalare immediatamente al Dirigente del Settore Informatica e innovazione qualsiasi evento o situazione, anche solamente sospetta, che possa compromettere il buon funzionamento del Sistema Informativo.

b) Tenere meticolosamente aggiornata la documentazione dell'infrastruttura di rete, dei sistemi e delle configurazioni, come anche l'inventario hardware e software.

c) Effettuare con la massima diligenza tutte le attività previste dal profilo di autorizzazione assegnato.

d) Pianificare e comunicare preventivamente all'utenza tutte le attività tecnico sistemistiche che possano compromettere la continuità operativa dei sistemi informatici.

e) Tutti i documenti riservati dei Sistemi Informativi devono essere sminuzzati con apposito dispositivo prima di essere gettati nella spazzatura.

f) Tutti i media o dispositivi di memorizzazione (cd, dvd, hard disk, nastri, penne usb, ecc.) devono essere formattati a basso livello, riscritti a livello di traccia o completamente distrutti prima di essere conferiti in discarica.

g) Ad ogni *logon* amministrativo deve corrispondere un *logout* anche nel caso di assenza temporanea; ad ulteriore sicurezza deve essere impostato lo *screen saver* protetto con password, con tempo di attivazione di 15 minuti.

h) Utilizzare sempre il livello di utente minimo necessario ad effettuare il compito amministrativo richiesto (non usare Administrator/root/Qsecofr se non necessario);

i) Le password di tutti gli amministratori di sistema, come già avviene per tutti gli utenti della rete, hanno validità di 3 (tre) mesi, a partire dalla loro creazione. Dopo questo periodo gli amministratori di sistema sono obbligati a sostituirle con altre nuove; per il lancio di servizi o di specifici compiti devono essere utilizzate utenze dedicate.

j) Gli Amministratore di Sistema esterni, che effettuano interventi presso l'Ente, possono collegarsi alla rete comunale direttamente con i propri dispositivi, solo con la supervisione dell'Amministratore interno dell'Ente.

k) Gli Amministratore di Sistema esterni, che effettuano interventi presso l'Ente, al completamento dell'attività, devono produrre un documento che attesti:

- data e ora di inizio e fine intervento
- dettaglio dell'attività svolta
- esito dell'intervento.

l) La sala macchine deve essere mantenuta pulita, ordinata, sgombra da qualsiasi oggetto o involucro non necessario.

5. ALLEGATO D – BIBLIOGRAFIA E SITOGRAFIA

Codice in materia di protezione dei dati personali [Testo consolidato vigente]
http://www.garanteprivacy.it/garante/doc.jsp?ID=1311248

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)
http://www.garanteprivacy.it/garante/doc.jsp?ID=1577499

Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema - 12 febbraio 2009 (G.U. n. 45 del 24 febbraio 2009)
http://www.garanteprivacy.it/garante/doc.jsp?ID=1591970

Amministratori di Sistema: avvio di una consultazione pubblica - 21 aprile 2009
(G.U. n. 105 dell' 8 maggio 2009)
http://www.garanteprivacy.it/garante/doc.jsp?ID=1611986