Comune di TARQUINIA

REGOLAMENTOSUI SOGGETTI CUI SONO AFFIDATI I PRIVILEGI DI AMMINISTRATORI DEL SISTEMA INFORMATICO

INDICE

ALLEGATI

Approvato con Deliberazione di Giunta n.230 del 28.12.2017

Comune di TARQUINIA	**REGOLAMENTO SUI SOGGETTI CUI SONO AFFIDATI I PRIVILEGI DI AMMINISTRATORI DEL SISTEMA INFORMATICO**	Versione 20171223

1. Oggetto

1 Il presente regolamento disciplina compiti, funzioni e responsabilità dei soggetti, interni e esterni all'Amministrazione, cui sono affidati i privilegi di amministratore del sistema informatico in attuazione di quanto previsto dalla Circolare AgID 18 aprile 2017, n° 2/2017 recante le Misure minime di sicurezza ICT per le Pubbliche Amministrazioni.

2. Soggetti cui sono affidati i privilegi di amministratore del sistema informatico: definizione e requisiti di nomina

2.1 L'amministratore di sistema, ovvero il soggetto cui sono affidati i privilegi di amministratore del sistema informatico (persona fisica), è la figura professionale che provvede alla gestione ed alla manutenzione di sistemi di elaborazione con particolare riferimento alla configurazione degli stessi. Nell'ambito dell'organizzazione è possibile individuare tipologie specifiche di amministratore di sistema, differenziate per livello di autorizzazione e profilo.

2.2 Si possono individuare amministratori di sistema interni o esterni all'organizzazione comunale.

2.3 L'attribuzione delle funzioni di gestore dei privilegi di amministratore del sistema informatico avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto della normativa in vigore sul trattamento dei dati e sulla sicurezza informatica.

3. Nomina dei soggetti interni cui sono affidati i privilegi di amministratore del sistema informatico

3.1 Il Sindaco, su proposta del Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale", provvede a nominare il soggetto o i soggetti, dipendenti dell'Amministrazione, a cui vengono affidati i privilegi di amministratore del sistema informatico assegnando il relativo profilo di autorizzazione.

3.2 La designazione deve essere comunque individuale e recare l'elencazione analitica degli ambiti di operatività sulla base del profilo di autorizzazione assegnato.

3.3 La designazione deve essere notificata per scritto ai soggetti individuati e dovrà in particolare individuare:

- **a)** dati identificativi del designato (nome, cognome, data e luogo di nascita, codice fiscale, residenza);
- **b)** ruolo e inquadramento nell'Amministrazione;
- **c)** profilo di autorizzazione assegnato;
- **d)** finalità dell'autorizzazione, con la specifica delle attività e dei compiti;
- **e)** l'ambito analitico di autorizzazione (fino a includere/escludere eventuali macchine, o insiemi di macchine, dispositivi, servizi, applicativi);
- **f)** riferimenti di posta elettronica e telefonici di reperibilità (per la sola gestione delle emergenze).

4. Nomina dei soggetti esterni cui sono affidati i privilegi di amministratore del sistema informatico

4.1 In caso di outsourcing, i soggetti esterni (persone fisiche) cui sono affidati i privilegi di amministratore del sistema informatico, sono designati dal titolare del servizio di outsourcing, nel rispetto di quanto definito all'articolo 2, comma 3.

4.2 In caso di designazione di soggetti esterni cui sono affidati i privilegi di amministratore del sistema informatico, il Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale" acquisisce dal soggetto esterno che opera in outsourcing, se persona giuridica, la seguente documentazione:

- copia della nomina della persona fisica ad amministratore di sistema e dei relativi profili di autorizzazione;
- dichiarazione circa il possesso da parte dei soggetti nominati dei requisiti di cui all'articolo 2;
- comunicazione decorrenza nomina;
- comunicazione revoca nomina.

4.3 A tutti i soggetti esterni cui sono affidati i privilegi di amministratore del sistema informatico si applicano gli articoli del presente regolamento.

5. Creazione del profilo di autorizzazione per i soggetti cui sono affidati i privilegi di amministratore del sistema informatico

5.1 I profili di autorizzazione sono descritti nell'allegato A al presente regolamento.

5.2 Per ciascuno dei soggetti cui sono affidati i privilegi di amministratore si provvede alla creazione degli account personali, associandovi il profilo di autorizzazione.

6. Elenco dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico

6.1 Gli estremi identificativi delle persone fisiche designate quali affidatari dei privilegi di amministratore del sistema informatico, sia interni che esterni, con l'indicazione dei compiti e delle funzioni ad essi attribuite devono essere riportati in un documento conservato ed aggiornato dal Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale". Nel documento devono essere riportate: la data della nomina e la data della revoca.

7. Compiti funzioni e responsabilità dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico

7.1 I compiti e le funzioni dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico nell'ambito del profilo di autorizzazione assegnato, descritto nell'allegato A sono, a titolo esemplificativo e non esaustivo:

a) monitorare l'infrastruttura informatica di competenza, anche attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
b) proporre l'introduzione ed integrazione di nuove tecnologie negli ambienti esistenti;
c) installare e configurare nuovo hardware/software sia lato client che lato server;
d) applicare le patch e gli aggiornamenti necessari al software di base applicativo, modificare la configurazione in base all'esigenze della Amministrazione;
e) gestire e mantenere aggiornati gli account utente relativi ai profili di autorizzazione;
f) fornire risposte a questioni tecniche di competenza sollevate dagli utenti;
g) affrontare e risolvere problemi, guasti o malfunzionamenti;
h) pianificare, eseguire e verificare la corretta esecuzione del backup e delle copie;
i) documentare le operazioni effettuate, le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni a problemi, guasti e malfunzionamenti;

j) ottenere le migliori prestazioni possibili con l'hardware a disposizione;
k) operare secondo le prescrizioni di sicurezza e le procedure previste dall'Amministrazione.

7.2 Ulteriori compiti e funzioni possono essere assegnati attraverso l'atto di nomina con cui vengono affidati i privilegi di amministratore del sistema informatico.

7.3 I soggetti cui sono affidati i privilegi di amministratore del sistema informatico sono personalmente responsabili della corretta esecuzione e dell'adempimento dei compiti e delle funzioni loro assegnate.

8. Registrazione degli accessi e degli eventi

8.1 Il sistema informatico deve integrare funzionalità di registrazione in appositi file di log degli accessi e di altre tipologie di eventi di sistema, prevedendo la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico.

8.2 Le registrazioni (*access log* e *system 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.

8.3 Le registrazioni devono comprendere i riferimenti temporali e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

8.4 Il Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale" provvede a controllare periodicamente, con cadenza almeno mensile, il file di log al fine di verificare il buon funzionamento dei sistemi e l'operato dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico.

8.5 È prevista la registrazione degli accessi logici da parte dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico ai sistemi client e alle workstation.

9. Esportazione e conservazione dei log

9.1 Il Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale", anche attraverso un soggetto cui sono affidati i privilegi di amministratore del sistema informatico, provvede ad esportare e conservare file contenenti i dati di log, di cui all'articolo 8, comma 1.

9.2 Il sistema informatico deve prevedere spazi adeguati di memorizzazione dei log; la capacità deve essere almeno doppia rispetto al massimo riscontrato tra una esportazione e la successiva.

9.3 Caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di log sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito software o con strumenti di esportazione e salvataggio.

9.4 E' necessario effettuare l'esportazione periodica, con cadenza almeno mensile, dei dati di log su supporti di memorizzazione non riscrivibili, riportando, anche con pennarello indelebile direttamente sul supporto, l'indicazione del periodo di riferimento, data di esportazione/salvataggio, tipologia di log su file LEGGIMI.TXT.

9.5 Nel caso fosse disponibile il servizio di certificazione della data, è consigliata l'apposizione di un *Timestamp digitale* direttamente alla cartella compressa dei log.

9.6 Non è esclusa la possibilità di implementazione di sistemi più sofisticati, come log server centralizzati, sempre che sia possibile certificare e firmare digitalmente i log.

9.7 I supporti di memorizzazione contenenti i file di log sono conservati in luogo sicuro a cura del Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale". L'accesso ai supporti di memorizzazione è precluso a tutto il personale interno e esterno, compresi i soggetti cui sono affidati i privilegi di amministratore del sistema informatico.

10. Sala Macchine

10.1 La sala macchine deve essere protetta con idonei strumenti di sicurezza fisica. Solo i soggetti cui sono affidati i privilegi di amministratore hanno facoltà di accedervi.

10.2 L'eventuale accesso di personale o di tecnici esterni è consentito previa identificazione, autorizzazione e registrazione da parte di un amministratore di sistema nominato e solamente sotto stretta sorveglianza di quest'ultimo.

10.3 L'accesso alla sala da parte di personale non autorizzato è vietato e di ciò deve essere dato avviso con idoneo cartello.

10.4 E' istituito il "Registro sala macchine" dove sono riportati, a cura di un amministratore di sistema nominato, gli eventi sensibili alla sicurezza, riservatezza integrità e disponibilità delle informazioni, come:

- installazioni/disinstallazioni/modifica delle configurazioni hardware o software;
- lavori di riparazione e di manutenzione;
- crash inattesi, interruzioni di servizio o di alimentazione;
- problemi agli impianti di alimentazione e climatizzazione;
- attivazione degli allarmi installati.

10.5 Ogni registrazione deve prevedere

a) il numero progressivo evento, distintamente per anno;
b) la data dell'evento/intervento;
c) una sintetica descrizione dell'evento/intervento;
d) il nominativo di chi ha effettuato l'intervento con indicazione di eventuali operatori e tecnici intervenuti.

11. Verifica attività e relazione annuale

11.1 Il Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale" verifica con cadenza almeno annuale l'operato dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico al fine di accertarne la conformità ai compiti attribuiti e controllare la rispondenza alle misure organizzative tecniche e di sicurezza previste dalle norme vigenti. Il risultato dell'operazione di verifica, sintetizzato in una relazione, viene inviato al Sindaco.

12. Procedura di revoca dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico

12.1 Il Sindaco, su proposta del Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale", revoca con atto scritto notificato al destinatario le funzioni di soggetto cui sono affidati i privilegi di amministratore del sistema informatico, nel caso di:

- inosservanza o inadempienza delle prescrizioni di sicurezza;
- violazione del presente Regolamento;
- sopravvenuta mancanza di requisiti (ai sensi dell'articolo 2 del presente regolamento);
- termine o modifica del rapporto contrattuale di lavoro del soggetto.

12.2 La revoca dell'incarico deve seguire la seguente procedura:

a) verifica dell'esistenza di servizi "lanciati" con l'account del soggetto da disabilitare;
b) assegnazione al servizio di un account per l'esecuzione della tipologia di servizi interessata;
c) controllo dell'eventuale presenza di backdoor (account o applicative, accessi remoti) riferibili al soggetto da disabilitare autorizzate o non autorizzate;
d) creare, nel caso non sia già esistente, un account amministrativo con lo stesso profilo del soggetto da disabilitare, da assegnare al nuovo soggetto (sostituto);
e) disabilitare l'account del soggetto revocato;
f) verificare che tutti i servizi collegati al profilo di autorizzazione del soggetto (sostituto) risultino perfettamente funzionanti;
g) comunicare la disabilitazione dell'account di soggetto cui sono affidati i privilegi di amministratore e la revoca dell'incarico alla persona fisica.

12.3 La revoca dei soggetti nominati secondo quanto prevede l'articolo 4 è compito del titolare del servizio di outsourcing che vi provvede nei casi previsti dal punto 12.1 e con le modalità di cui al punto 12.2.

13 – Divieti e disposizioni

13.1 La documentazione interna del sistema informatico dell'Ente, in particolare quella relativa all'infrastruttura di rete, alla configurazione dei sistemi e degli applicativi, alle impostazioni o abilitazioni degli utenti è conservata in luogo sicuro, preferibilmente non accessibile in rete.

13.2 L'accesso alla documentazione di cui al punto precedente è consentito esclusivamente ai soggetti cui sono affidati i privilegi di amministratore per la consultazione e aggiornamento.

13.3 È fatto divieto di trasportare la documentazione di cui al punto 13.1 fuori dalla sede dell'Ente in qualsiasi formato o supporto. 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.

13.4 Gli account e le relative credenziali di livello amministratore di sistema sono segrete e non devono essere rivelate ad alcuno per nessun motivo. E' fatto divieto di trasmettere in qualsiasi formato anche criptato dette informazioni.

13.5 In caso di perdita di segretezza di una credenziale di livello amministratore di sistema il soggetto cui sono affidati i privilegi di amministratore deve comunicare tempestivamente l'evento al Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale"; è altresì necessario annotare l'evento nel registro degli incidenti alla sicurezza,

effettuarne tempestivamente la modifica e verificare che non siano stati creati nel frattempo nuovi utenti o modificati profili di autorizzazione.

13.6 Qualora giungano richieste telefoniche da parte dell'Autorità Giudiziaria o degli organi di Polizia è necessario richiedere l'identità del chiamante; si provvederà a richiamare non direttamente l'interno, avendo così la certezza sull'identità del richiedente (call-back).

13.7 Prima di collegare un nuovo apparato alla rete il Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale", provvede a sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.

13.8 Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. Se per l'autenticazione si utilizzano certificati digitali, le chiavi private devono essere adeguatamente protette.

13.9 Quando l'autenticazione a più fattori non è supportata, il Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale" provvede ad utilizzare per le utenze amministrative credenziali di elevata robustezza (almeno 14 caratteri).

13.10 Il Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale" provvede ad adottare opportuni accorgimenti tecnici affinché le credenziali amministrative vengano sostituite con sufficiente frequenza e per impedire che le credenziali già utilizzate possano essere utilizzate a breve distanza di tempo.

13.11 Il Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale" provvede a che le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, siano utilizzate solo per le situazioni di emergenza e le relative credenziali siano gestite in modo da assicurare l'imputabilità di chi ne fa uso.

13.12 Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati, da un soggetto cui sono affidati i privilegi di amministratore, utilizzando la configurazione standard.

13.13 In Allegato C sono riportate le "Linee guida e note operative" specifiche per gli Amministratori di Sistema.

14 Disposizioni finali

14.1 Il presente regolamento entra in vigore dalla data di esecutività del provvedimento di approvazione

Comune di TARQUINIA	**REGOLAMENTO SUI SOGGETTI CUI SONO AFFIDATI I PRIVILEGI DI AMMINISTRATORI DEL SISTEMA INFORMATICO**	Versione 20171223

ALLEGATO A

TIPOLOGIA DI AMMINISTRATORE E PROFILI DI AUTORIZZAZIONE

Livello sicurezza	RUOLO	PROFILO DI AUTORIZZAZIONE
0	**AMMINISTRATORE GENERALE DI DOMINIO** Livello più alto di autorizzazione nell'ambito del singolo dominio della rete dell'organizzazione	Autorizzato • all'accesso completo a tutti i dati e a tutti gli apparati appartenenti ad un singolo dominio della rete • alla creazione degli *account* e all'abilitazione agli accessi agli amministratori di livello 1 e 2 del solo dominio di appartenenza • all'analisi e controllo dei log di tutte le macchine appartenenti al solo dominio di appartenenza e degli apparati
1	**AMMINISTRATORE SERVER** Amministratore di un singolo sistema server	Autorizzato • all'accesso completo al sistema e ai dati contenuti nel server • a compiere qualsiasi operazione sistemistica e di modifica della configurazione del server • all'analisi e controllo dei log
1	**AMMINISTRATORE DEGLI ACCOUNT** Amministratore degli *account* utente per il solo dominio di appartenenza	Autorizzato • alla creazione/disabilitazione degli account utenti; • all'assegnazione del profilo di autorizzazione dell'account utente.
1	**AMMINISTRATORE INFRASTRUTTURA DI RETE** Amministratore dell'infrastruttura di rete e di comunicazione	Autorizzato • all'accesso completo ai dispositivi di comunicazione (es router, switch, hub, centrale telefonica) e alle linee di comunicazione; • a compiere qualsiasi operazione di modifica della configurazione di dispositivi di comunicazione.;
1	**AMMINISTRATORE DEI DISPOSITIVI DI SICUREZZA**	Autorizzato • all'accesso completo ai dispositivi di sicurezza (es Firewall, antivirus, log management) • a compiere qualsiasi operazione di modifica della configurazione dei dispositivi di sicurezza.;
1	**AMMINISTRATORE DI UN DATA BASE**	Autorizzato • all'accesso completo al motore del database e ai dati memorizzati, • a compiere qualsiasi operazione di modifica degli schemi di data base .;
1	**AMMINISTRATORE DEI BACKUP E DELLE REPLICHE DEI DATI**	Autorizzato all'accesso (in lettura): • di *dump* dei data base; • delle *share* di rete; • dei *system state* e degli *snapshot* delle macchine; • delle configurazioni (soggette a backup)
2	**AMMINISTRATORE DI UN SINGOLO SERVIZIO O APPLICAZIONE**	Autorizzato: • alla gestione modifica delle configurazioni, stop/start del singolo servizio o applicazione
2	**AMMINISTRATORE LOCALE DI SINGOLI SISTEMI CLIENT**	Autorizzato • all'accesso completo ad un insieme specificato nella nomina di sistemi *client* ed ai dati contenuti nei dispositivi

ALLEGATO B

MODELLO MODULO NOMINA DEI SOGGETTI A CUI VENGONO AFFIDATI I PRIVILEGI DI AMMINISTRATORE DEL SISTEMA INFORMATICO

In conformità alla normativa vigente ed in particolare a quanto prevedono le "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni " di cui alla Circolare AgID 18 aprile 2017, n° 2/2017 ed al "Regolamento sui soggetti cui sono affidati i privilegi di amministratori del sistema informatico nel comune di TARQUINIA", allegato in copia al presente atto, accertato il possesso dei requisiti di cui all'articolo 2 del citato Regolamento, con la presente

IL_____

NOMINA

Il sig.
Cognome e nome

Codice fiscale

Data e luogo di nascita

Luogo di residenza

Funzione

Area settore di appartenenza

Recapiti telefonici (solo per gestione emergenze)

QUALE SOGGETTO A CUI VENGONO AFFIDATI I PRIVILEGI DI AMMINISTRATORE DEL SISTEMA INFORMATICO DEL COMUNE DI TARQUINIA PER LA/LE TIPOLOGIE E PROFILO/PROFILI DI AUTORIZZAZIONE DI SEGUITO DESCRITTI

RUOLO	PROFILO DI AUTORIZZAZIONE
0 AMMINISTRATORE GENERALE DI DOMINIO Livello più alto di autorizzazione nell'ambito del singolo dominio della rete dell'organizzazione	Autorizzato • all'accesso completo a tutti i dati e a tutti gli apparati appartenenti ad un singolo dominio della rete • alla creazione degli *account* e all'abilitazione agli accessi agli amministratori di livello 1 e 2 del solo dominio di appartenenza • all'analisi e controllo dei log di tutte le macchine appartenenti al solo dominio di appartenenza e degli apparati
0 AMMINISTRATORE SERVER Amministratore di un singolo sistema server	Autorizzato • all'accesso completo al sistema e ai dati contenuti nel server • a compiere qualsiasi operazione sistemistica e di modifica della configurazione del server • all'analisi e controllo dei log
0 AMMINISTRATORE DEGLI ACCOUNT Amministratore degli account per il solo dominio di appartenenza	Autorizzato • alla creazione/disabilitazione degli account utenti; • all'assegnazione del profilo di autorizzazione dell'account utente.
0 AMMINISTRATORE INFRASTRUTTURA DI RETE	Autorizzato • all'accesso completo ai dispositivi di comunicazione (es router, switch, hub, centrale telefonica) e alle linee di comunicazione; • a compiere qualsiasi operazione di modifica della configurazione di

Amministratore dell'infrastruttura di rete e di comunicazione	dispositivi di comunicazione.;
0 AMMINISTRATORE DEI DISPOSITIVI DI SICUREZZA	Autorizzato • all'accesso completo ai dispositivi di sicurezza (es Firewall, antivirus, log management) • a compiere qualsiasi operazione di modifica della configurazione dei dispositivi di sicurezza.;
0 AMMINISTRATORE DI UN DATA BASE	Autorizzato • all'accesso completo al motore del database e ai dati memorizzati, • a compiere qualsiasi operazione di modifica degli schemi di data base .;
0 AMMINISTRATORE DEI BACKUP E DELLE REPLICHE DEI DATI	Autorizzato all'accesso (in lettura): • di *dump* dei data base; • delle *share* di rete; • dei *system state* e degli *snapshot* delle macchine; • delle configurazioni (soggette a backup)
0 AMMINISTRATORE DI UN SINGOLO SERVIZIO O APPLICAZIONE	Autorizzato: • alla gestione modifica delle configurazioni, stop/start del singolo servizio o applicazione
0 AMMINISTRATORE LOCALE DI SINGOLI SISTEMI CLIENT	Autorizzato • all'accesso completo ad un insieme specificato nella nomina di sistemi *client* ed ai dati contenuti nei dispositivi

Ai sensi della presente nomina Lei è tenuto al rispetto delle disposizioni di cui al sopra citato Regolamento ed ai seguenti adempimenti ed obblighi:

- informare tempestivamente il Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale" di tutte le questioni rilevanti ai fini di legge ed in termini di sicurezza;
- agire in modo da mantenere il segreto e la riservatezza sui dati personali dei quali è venuto a conoscenza nello svolgimento delle operazioni cui è autorizzato;
- non comunicare o diffondere informazioni eventualmente acquisite durante la permanenza nei locali dell'Ente;
- non utilizzare documenti, dati ed informazioni acquisite durante le attività svolte nell'espletamento delle operazioni cui è incaricato per finalità che neon siano ricomprese fra quelle per le quali è autorizzato;
- non comunicare o diffondere, senza la preventiva autorizzazione del Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale", le informazioni relative alla situazione di sicurezza della dell'organizzazione (sistemi operativi, applicativi software, documentazione su architettura e connessioni di rete; misure e organizzazione della sicurezza),
- eseguire puntualmente tutte le istruzioni impartite dal Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale";
- ……

Si ricorda che le attività da Lei svolte, descritte nella presente nomina, saranno oggetto di controllo, in conformità alla normativa vigente ed a quanto stabilito dal Regolamento.

Luogo _____ DATA_____

Il Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale"

Il Sindaco

Per presa visione e accettazione di tutte le condizioni
L'amministratore di sistema

ALLEGATO C – LINEE GUIDA E NOTE OPERATIVE

1. Attenersi scrupolosamente a tutte le procedure operative e segnalare immediatamente al Responsabile del Settore da cui dipende l'Ufficio "Sistema informativo comunale" qualsiasi evento o situazione, anche solamente sospetta, che possa compromettere il buon funzionamento del sistema informatico.
2. Tenere meticolosamente aggiornata la documentazione dell'infrastruttura di rete, dei sistemi e delle configurazioni, come anche l'inventario hardware e software.
3. Effettuare con la massima diligenza tutti i controlli inclusi nelle procedure operative.
4. Pianificare e comunicare preventivamente all'utenza tutte le attività tecnico sistemistiche che possano compromettere la continuità operativa dei sistemi informatici.
5. Tutti i documenti dei sistemi informativi devono essere sminuzzati con apposito dispositivo prima di essere gettati nella spazzatura.
6. 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.
7. In caso di invio di un media in assistenza tecnica o in riparazione, assicurarsi che sia realmente illeggibile.
8. 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 inferiori ai 5 minuti.
9. Utilizzare sempre il livello di utente minimo necessario ad effettuare il compito amministrativo richiesto;
10. Cambiare le password relative ad account amministrativi di livello 2 ogni 3 mesi e le password amministrative di livello più alto almeno ogni mese; per il lancio di servizi o di specifici compiti utilizzare solamente utenze dedicate, con possibilità di modifica della password ad intervalli semestrali.
11. Al personale di supporto esterno, anche se nominato amministratore di sistema, è vietato il collegamento alla rete o direttamente ai dispositivi dell'Ente, di qualsiasi strumento non di proprietà dell'organizzazione (ad esempio notebook, penne usb, ecc.).