ALL. 1

ALLEGATO ALLA
DETERMINA N. 22/AS
DEL 15 GEN. 2014

REGOLAMENTO
DEGLI AMMINISTRATORI DI SISTEMA
DELL'ASUR MARCHE

"Quis custodiet ipsos custodes?"
Giovenale (VI Satira)

Sommario Pag.

Art. 1 - Oggetto

Il presente Regolamento disciplina compiti, funzioni e responsabilità degli Amministratori di sistema interni ed esterni all'Azienda Sanitaria Unica Regionale delle Marche, in attuazione di quanto previsto dal Codice in materia di protezione dei dati personali (D.lgs. 30 giugno 2003, n. 196 e ss.mm.ii.), dal Disciplinare tecnico in materia di misure minime di sicurezza di cui all'Allegato B al medesimo Codice e, da ultimo, dal provvedimento a carattere generale dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008, denominato "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", così come modificato con successivo provvedimento del 25 giugno 2009.

Art. 2 – Amministratore di Sistema – Definizione e requisiti di nomina

1. Amministratore di sistema, in ambito informatico, è la figura professionale che si occupa della gestione e della manutenzione di sistemi di elaborazione e delle sue componenti. Ai fini del presente regolamento sono considerati tali anche altre figure professionali che si occupano di sistemi di gestione delle basi di dati, di sistemi software complessi, delle reti locali e degli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

2. L'attribuzione delle funzioni di Amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato (intese come qualità tecniche, professionali e di condotta), il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati ivi compreso il profilo relativo alla sicurezza.

3. Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice Privacy, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29 del Codice privacy.

Art. 3 - Nomina diretta degli Amministratori di sistema

1. Il Direttore Generale dell'ASUR, Titolare del trattamento dei dati personali provvede, sentito il Responsabile dei Sistemi Informativi aziendale, a nominare l'Amministratore di sistema competente a livello centrale, assegnando il relativo profilo di autorizzazione, come previsto nell'Allegato A al presente Regolamento.

2. I Direttori di Area Vasta, delegati per l'effetto in forza del presente regolamento, provvedono, per l'ambito di rispettiva competenza:

- alla nomina dei Responsabili dei Sistemi Informativi di Area Vasta quali Amministratori di Sistema, assegnando il relativo profilo di autorizzazione, come previsto nell'allegato A al presente Regolamento;
- alla nomina, su proposta dei Responsabili dei Sistemi Informativi di Area Vasta, di altri Amministratori di Sistema, assegnando il relativo profilo di autorizzazione, come previsto nell'allegato A del presente Regolamento.

4. La designazione quale Amministratore di sistema deve essere, in ogni caso, individuale e recare l'elencazione analitica degli ambiti di operatività sulla base del profilo di autorizzazione assegnato.

5. La designazione dovrà essere notificata per iscritto ai soggetti individuati e dovrà indicare, in particolare:

a) nome e cognome, codice fiscale, data e luogo di nascita, residenza dell'Amministratore di Sistema nominato;
b) funzione ed Area organizzativa di appartenenza;
c) la tipologia di Amministratore di sistema ed il profilo di autorizzazione affidato (domain, server, networking, backup, come riportato in *Allegato A*);
d) le finalità dell'autorizzazione, con la specifica delle attività e dei compiti (gestione backup, gestione del dominio e degli account, ecc);
e) l'ambito analitico di autorizzazione (fino a includere/escludere eventuali macchine o insiemi di macchine, dispositivi, servizi, applicativi);
f) i riferimenti telefonici dell'Amministratore di sistema nominato (per la sola gestione delle emergenze).

Art. 4 - Nomina indiretta degli Amministratori di sistema

In caso di outsourcing, i Responsabili esterni del trattamento dei dati personali, designati dal Direttore Generale e, nell'ambito della delega loro conferita, dai Direttori di Area Vasta, possono nominare Amministratori di sistema esterni.

In caso di nomina indiretta, i Responsabili dei Sistemi Informativi - aziendali e di Area Vasta - acquisiscono dai Responsabili esterni del trattamento dei dati personali la seguente documentazione:

- dichiarazione circa il possesso da parte dei nominati dei requisiti di cui all'art. 2;
- copia della nomina della persona fisica quale Amministratore di Sistema;
- l'elenco degli Amministratori di sistema che gestiscono i trattamenti;
- dichiarazione sull'adempimento dell'obbligo di formazione degli Amministratori nominati, secondo quanto previsto dalla normativa sulla privacy.

3. A tutti gli Amministratori di sistema esterni si applicano gli articoli del presente Regolamento.

Art. 5 – Creazione del profilo per gli Amministratori di sistema

1. I Responsabili dei Sistemi Informativi Aziendale e di Area Vasta provvedono alla creazione degli account personali di ogni Amministratore di sistema designato per il rispettivo ambito territoriale, associandovi il profilo di autorizzazione (*Allegato A - Tipologia di Amministratore e profili di autorizzazione*).

Art. 6 - Elenco degli Amministratori di sistema

1. Gli estremi identificativi delle persone fisiche designate quali Amministratori di sistema, sia interni che esterni, con l'elenco dei compiti e delle funzioni ad essi attribuite, devono essere riportati in un documento interno, conservato ed aggiornato a cura dei Responsabili dei Sistemi Informativi - aziendale e di Area Vasta.

2. L'identità degli Amministratori di sistema, la cui attività riguarda anche indirettamente servizi o sistemi che trattano informazioni di carattere personale dei dipendenti, è resa nota

nei rispettivi siti intranet aziendali e territoriali, a cura dei rispettivi Responsabili dei Sistemi Informativi – aziendale e di Area Vasta.

Art. 7 – Compiti, funzioni e responsabilità degli Amministratori di sistema

1. I compiti e le funzioni degli Amministratori di Sistema in base ai ruoli assegnati, nell'ambito dei profili di autorizzazione individuati nell'*Allegato A*) al presente Regolamento, sono, a titolo esemplificativo e non esaustivo :

a) monitorare l'infrastruttura informatica di competenza attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
b) introdurre ed integrare nuove tecnologie negli ambienti esistenti;
c) installare e configurare nuovo hardware/software sia lato client sia lato server;
d) applicare le patch e gli aggiornamenti necessari al software di base ed applicativo,
e) modificare le configurazioni in base alle esigenze dell'organizzazione;
f) gestire e tenere aggiornati gli account utente ed i relativi profili di autorizzazione;
g) fornire risposte alle questioni tecniche sollevate dall'utenza;
h) porre rimedio ai problemi/guasti tramite tecniche di *troubleshooting*;
i) pianificare e verificare la corretta esecuzione dei backup e delle repliche;
j) 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;
k) ottenere le migliori prestazioni possibili con l'hardware a disposizione;
l) operare secondo le prescrizioni di sicurezza e le procedure interne previste.

2. Gli Amministratori di sistema sono personalmente responsabili della corretta esecuzione e dell'adempimento dei compiti e funzioni loro assegnate.

Art. 8 - Registrazione degli accessi e degli eventi

1. Ogni sistema informatico registra in appositi file di log gli eventi di sistema: accensione, chiusura, logon utenti, errori, ecc. L'Amministratore di sistema controlla periodicamente i file di log per verificare il buon funzionamento dei sistemi.

2. Devono essere registrati gli accessi (login) ai sistemi di elaborazione ed agli archivi elettronici effettuati dagli Amministratori di sistema.

3. Le registrazioni (*access log e system log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità.

4. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo non inferiore a 6 mesi.

5. E' prevista, altresì, la registrazione degli accessi logici da parte degli Amministratori di Sistema ai sistemi client e workstation.

6. Nei casi più semplici la registrazione degli accessi logici può essere effettuata tramite funzionalità già disponibili nei più diffusi sistemi operativi, senza richiedere necessariamente l'uso di strumenti *software* o *hardware* aggiuntivi. Per esempio, la registrazione locale dei dati di accesso su una postazione, in determinati contesti, può essere ritenuta idonea al corretto adempimento qualora goda di sufficienti garanzie di integrità.

7. Con valutazione del titolare dovrà essere considerata l'idoneità degli strumenti disponibili oppure l'adozione di strumenti più sofisticati, quali la raccolta dei *log* centralizzata e di tecniche crittografiche per la verifica dell'integrità delle registrazioni.

8. Con valutazione del titolare dovrà essere considerata l'eventualità di firmare digitalmente i file di log, anche in formato compresso.

Art. 9 - Conservazione ed Esportazione dei log

1. E' necessario effettuare l'esportazione dei dati di log su supporti di memorizzazione non riscrivibili, con cadenza almeno mensile. Tali supporti riporteranno le seguenti informazioni:

- periodo di riferimento;
- data di salvataggio;
- tipologia di log su file LEGGIMI.TXT ed anche direttamente sul supporto con pennarello indelebile.

3. I supporti di memorizzazione contenenti i file di log sono conservati a cura dei Responsabili dei Sistemi Informativi - Aziendale e di Area Vasta - in un contenitore chiuso a chiave. L'accesso è precluso a tutto il personale interno ed esterno, inclusi gli Amministratori di Sistema medesimi.

4. I sistemi informatici ed i dispositivi di comunicazione devono prevedere spazi adeguati di memorizzazione dei log, con capacità almeno doppia rispetto al massimo riscontrato tra una esportazione e la successiva.

Art. 10 - Sala Macchine

1. La Sala Macchine è considerata "zona di massima sicurezza". Solo gli Amministratori di sistema nominati hanno facoltà di accesso. L'accesso al personale non autorizzato è vietato e devono essere apposti cartelli di avvertimento, come riportato nell'*Allegato C – Cartellonistica.*

2. La Sala Macchine è chiusa a chiave e protetta da adeguati sistemi di sicurezza fisica ed ogni singolo accesso ad essa da parte degli Amministratori di sistema è registrato.

4. L'ingresso di eventuali tecnici esterni deve prevedere la loro identificazione, autorizzazione e registrazione. In ogni caso, l'accesso di personale esterno è autorizzato solamente sotto stretta sorveglianza di un Amministratore di Sistema nominato.

Art. 11 - Libro di bordo Sala Macchine – *Logbook*

1. Presso le Sedi operative di ciascuna Area Vasta è istituito, compatibilmente con l'organizzazione interna, il "Libro di bordo Sala Macchine" o "*Logbook* Sala Macchine", dove sono riportati tutti gli eventi sensibili alla riservatezza, integrità e disponibilità delle informazioni.

2. Nel "*Logbook* Sala Macchine" devono essere riportate le seguenti circostanze:
   a) Registrazione accessi sala macchine di personale interno ed esterno;
   b) Installazioni/Disinstallazioni/Modifica delle configurazioni hardware o software;

c) Lavori di riparazione e di manutenzione;
d) Riavvii attesi, crash inattesi, interruzioni di servizio o di alimentazione;
e) Problemi agli impianti di comunicazione, alimentazione, protezione, antincendio e climatizzazione nonché l'attivazione degli allarmi (intrusione, temperatura, allagamento).

ed 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 sul funzionamento degli apparati della sala macchina (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 ed eventuali note.

Art. 12 - Formazione ed aggiornamento

I Responsabili dei Sistemi Informativi - aziendale e di Area Vasta - promuovono, con cadenza almeno annuale, la formazione e l'aggiornamento degli Amministratori di sistema in materia di sicurezza informatica.

Art. 13 - Verifica delle attività e relazione annuale

1. I Responsabili dei Sistemi Informativi - aziendale e di Area Vasta – verificano, rispettivamente per conto del Direttore Generale e dei Direttori di Area Vasta, con cadenza almeno annuale, l'operato degli Amministratori di sistema, al fine di accertarne la conformità alle mansioni attribuite e controllare la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti.

2. Il Responsabile aziendale dei Sistemi Informativi verifica, per conto del Direttore Generale e con medesima cadenza annuale, l'operato dei Responsabili dei Sistemi Informativi di Area Vasta che siano stati nominati dal relativo Direttore ai sensi dell'art.3, comma 2, del presente Regolamento.

3. I Responsabili dei Sistemi Informativi - aziendale e di Area Vasta - comunicano al Direttore Generale ed ai Direttori di Area Vasta eventuali comportamenti non conformi al presente Regolamento da parte degli Amministratori di sistema designati, proponendone la revoca qualora ricorrenti le ipotesi di cui all'art. 14.

Art. 14 - Procedura di revoca degli Amministratori di Sistema

1. Il Direttore Generale ed i Direttori di Area Vasta, su proposta motivata dei Responsabili dei Sistemi Informativi – aziendale e di Area vasta - revocano con atto scritto notificato al destinatario le funzioni di Amministratore di Sistema in caso di:

- inadempienza o inosservanza delle prescrizioni di sicurezza;
- violazione del presente Regolamento;

- sopravvenuta mancanza dei requisiti ai sensi dell'art. 2 del presente Regolamento;
- modifica del rapporto contrattuale di lavoro dell'Amministratore di Sistema.

2. La revoca dell'incarico di un Amministratore di Sistema dovrà seguire in modo rigoroso e specifico, nell'ordine, la seguente procedura:

a) verificare l'esistenza di eventuali servizi lanciati con l'account dell'Amministratore di Sistema da disabilitare;
b) assegnare al servizio un account specifico per l'esecuzione della tipologia di servizi interessata;
c) controllare l'esistenza di eventuali backdoor (account o applicative, accessi remoti, autorizzate o non autorizzate) riferibili all'Amministratore di Sistema da disabilitare;
d) 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);
e) disabilitare l'account dell'Amministratore di Sistema revocato;
f) verificare che tutti i servizi collegati al profilo di autorizzazione dell'Amministratore di Sistema risultino perfettamente funzionanti;
g) comunicare la disabilitazione dell'account di Amministratore di Sistema e la revoca dell'incarico alla persona fisica.

3. La revoca degli Amministratori di sistema esterni nominati, ai sensi dell'art. 4 del presente Regolamento, è compito del Responsabile esterno del trattamento, che vi provvede nei casi e secondo i criteri di cui di cui ai commi 1 e 2 del presente articolo, nonché su richiesta motivata dei Responsabili dei Sistemi Informativi - aziendale e di Area Vasta.

Art. 15 - Divieti e disposizioni

1. La documentazione interna dei Sistemi Informativi, in particolare la documentazione relativa all'infrastruttura di rete, alla configurazione dei sistemi o degli applicativi, alle impostazioni o abilitazioni degli utenti, è conservata in luogo sicuro.

2. L'accesso a detta documentazione è consentito solamente agli Amministratori di Sistema, per il solo tempo necessario alla consultazione ed all'aggiornamento.

3. E' vietato trasportare la documentazione interna dei Sistemi Informativi all'esterno dell'Azienda Sanitaria Unica Regionale in qualsiasi formato o supporto.

4. Gli *account* e le relative password di livello Amministratore di Sistema sono segrete e non devono essere rivelate a nessuno. E' vietato trasmettere in qualsiasi formato anche criptato dette informazioni.

5. In caso di perdita di segretezza di una password di livello Amministratore di Sistema, è necessario comunicare tempestivamente l'evento ai Responsabili dei Sistemi Informativi - aziendale e di Area Vasta - i quali provvederanno alla modifica e alla verifica in merito all'eventuale creazione di utenti o alla modifica di profili di autorizzazione.

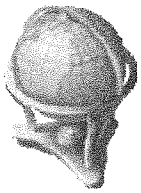
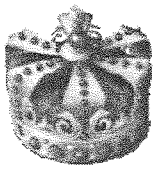
Art. 16 – Abrogazione e rinvio

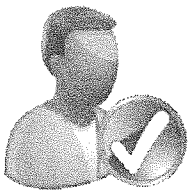
1. Dalla data di entrata in vigore del presente Regolamento sono abrogate tutte le disposizioni regolamentari in contrasto a quanto prescritto.

2. Per tutto quanto non previsto nel presente Regolamento, si fa esplicito rinvio alla vigente normativa e regolamentazione in materia, con particolare riferimento alle norme del Codice per la protezione dei dati personali e ai provvedimento dell'Autorità Garante per la protezione dei dati personali.

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'organizzazione. 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.
Domain Administrator 	0	Livello più alto di autorizzazione nell'ambito del singolo Dominio della rete dell'organizzazione. 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.
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 di comunicazione (es. router, switch, hub, centrale telefonica) ed alle linee di comunicazione; 2. a compiere qualsiasi operazione di modifica della configurazione dei dispositivi di comunicazione; 3. all'analisi e controllo dei log, del traffico dati e telefonico.
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.

Allegato B

Fac – simile di nomina quale 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) recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle relative funzioni" ed al Regolamento aziendale concernente gli Amministratori di Sistema, approvato con determina n. ... / ASURDG del ..., allegato in copia al presente atto, accertato il possesso dei requisiti di cui all'art. 2 del citato Regolamento, con la presente

SI NOMINA la S.V.

Cognome e nome: _____

Codice fiscale: _____

Data e luogo di nascita: _____

Luogo di residenza:_____

Funzione: _____

Area organizzativa di appartenenza: _____

Recapiti telefonici:_____(solo per gestione emergenze)

Quale "Amministratore di Sistema" per la/le tipologia/tipologie e profilo/profili di autorizzazione di seguito descritti.

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.
❑ 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 di comunicazione (es. router, switch, hub, centrale telefonica) ed alle linee di comunicazione;

	2. a compiere qualsiasi operazione di modifica della configurazione dei dispositivi di comunicazione; 3. all'analisi e controllo dei log, del traffico dati e telefonico.
❑ 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.

Ai sensi della presente nomina, la S.V. è tenuta al rispetto delle disposizioni di cui al sopra citato Regolamento aziendale concernente gli Amministratori di Sistema, nonché ai seguenti adempimenti ed obblighi:

a) informare prontamente il Responsabile dei Sistemi Informativi di tutte le questioni rilevanti ai fini di legge ed in termini di sicurezza;
b) mantenere il segreto e la riservatezza sui dati personali conosciuti o ai quali abbia avuto accesso nello svolgimento delle prestazioni contrattuali;
c) non comunicare a nessuno le eventuali informazione acquisite durante la permanenza negli uffici aziendali;
d) non utilizzare i dati trattati e le informazioni acquisite per finalità che non siano strettamente inerenti la funzione svolta;
e) osservare la massima riservatezza in merito alle informazioni ottenute nello svolgimento dell'attività professionale, incluse le informazioni relative alla situazione di sicurezza dell'organizzazione, come sistemi operativi, applicativi software, documentazione, architettura e connessioni di rete;
f) attenersi, in ogni caso, a tutte le istruzioni che saranno impartite dal Responsabile dei Sistemi Informativi.

Si ricorda alla S.V. che il provvedimento del Garante già citato, obbliga l'azienda alla "verifica" almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Sulla base di quanto previsto al punto 4.3, del citato Provvedimento del Garante, si informa gli estremi identificativi della S.V. con l'elenco delle funzioni attribuite, saranno riportati in un documento interno conservato agli atti.

Luogo _____ Data _____

Per presa visione ed accettazione di tutte le condizioni

Il Direttore Generale /Direttore di AV

_____

L'Amministratore di Sistema

_____

Allegato C - Cartellonistica