ALLEGATO alla DELIBERA N. 090 DEL 04 AGO.2017

REGOLAMENTO CONCERNENTE LA NOMINA, LE FUNZIONI ED I COMPITI DEGLI AMMINISTRATORI DI SISTEMA DELL'ASP di CROTONE

INDICE

Articolo 1 - Scopo del Regolamento

Con Provvedimento del 27 Novembre 2008 recante "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", così come modificato dal Provvedimento del 25 giugno 2009, il Garante per la protezione dei dati personali ha definito AMMINISTRATORI di SISTEMA (ADS), tutte quelle "*figure professionali dedicate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti*".

Ai fini del suddetto provvedimento vengono però considerate tali anche altre figure 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 gli amministratori di sistemi software complessi*".

Rientrano in questa accezione ampia di AMMINISTRATORE DI SISTEMA tutte quelle figure chiamate a svolgere le funzioni richiamate nel "*Disciplinare tecnico in materia di misure*

minime di sicurezza", di cui all'ALLEGATO B al D.lgs. n.ro 196/2003 (Artt. da 33 a 36 del Codice) e, più in generale, che comportano la concreta capacità di accedere, in modo privilegiato, a risorse del sistema informativo e a dati personali (anche qualora non siano preposte a operazioni che implicano una comprensione del dominio applicativo), e nella misura in cui sono, nelle loro consuete attività tecniche, responsabili di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali:

- realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati);
- organizzazione dei flussi di rete;
- gestione dei supporti di memorizzazione;
- custodia delle credenziali di autenticazione e di autorizzazione;
- gestione dei sistemi di autenticazione e di autorizzazione;
- manutenzione hardware.

Possono dunque qualificarsi quale Amministratori di Sistema i seguenti soggetti:

- amministratori di sistemi di autenticazione;
- amministratori di server;
- amministratori di apparati rete;
- amministratori di base di dati;
- amministratori di apparati di sicurezza;
- amministratori di applicazioni.

Ciò posto, il Garante, nel segnalare a tutti i TITOLARI di trattamenti di dati personali, soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici, la particolare criticità del ruolo degli amministratori di sistema, richiama l'attenzione dei medesimi TITOLARI sulla necessità di adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di amministratore di sistema; richiama, inoltre, l'attenzione sull'esigenza di VALUTARE con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali.

Si consideri, inoltre, che in attuazione di quanto previsto dalla Direttiva del 1 agosto 2015 del Presidente del Consiglio dei Ministri, l'Agenzia per l'Italia Digitale (AGID) ha emesso, in data 26 Aprile 2016, le MISURE MINIME DI SICUREZZA ICT a cui tutte le pubbliche amministrazioni devono allinearsi.

Il documento anticipa le *Regole Tecniche per la Sicurezza Informatica delle PA* (la cui emanazione è competenza del Dipartimento della Funzione Pubblica), con l'obiettivo di fornire tempestivamente un riferimento utile a stabilire se il livello di protezione dei sistemi ICT delle pubbliche amministrazioni risponde alle esigenze operative di messa in sicurezza dei sistemi, individuando anche gli interventi idonei al suo adeguamento.

Vengono pertanto introdotti dei controlli denominati ABSC (AgID Basic Security Controls) che dovrebbero essere implementati per ottenere un determinato livello di sicurezza. Si identificano 3 livelli:

- "Minimo", al di sotto il quale nessuna amministrazione può scendere;
- "Standard", che costituisce la base di riferimento nella maggior parte dei casi;
- "Alto", che potrebbe essere un obiettivo a cui tendere.

Vengono delineate 8 classi di controlli, tra cui il controllo ABSC5 (CSC5) "*Uso appropriato dei privilegi di amministratore: Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi*".

In considerazione di tutto quanto sopra e di quanto previsto dal NUOVO REGOLAMENTO EUROPEO (UE) 2016/679 concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, entrato in vigore il 24 Maggio 2016, e che diverrà applicabile in tutti gli Stati membri a partire dal 25 Maggio 2018, il presente REGOLAMENTO ha lo scopo di delineare e dettare *le procedure di nomina e di attribuzione delle funzioni degli amministratori di sistema dell'ASP di Crotone*, nonché gli adempimenti in materia di protezione dei dati personali e, in particolare, l'adozione di specifiche MISURE e CAUTELE in riferimento alle mansioni svolte dagli amministratori di sistema e dai soggetti ad essi assimilabili.

Articolo 2 - Definizioni

- **Dati personali**: qualunque informazione relativa ad un soggetto - persona fisica, persona giuridica, ente od associazione - identificato o identificabile (anche indirettamente, mediante riferimento a qualsiasi altra informazione, compreso un numero di identificazione personale).
- **Trattamento**: qualunque operazione, o complesso di operazioni, effettuato sui dati personali (raccolta, registrazione, organizzazione, conservazione; consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo. interconnessione, blocco comunicazione, diffusione, cancellazione, distruzione di dati). Rientrano nella

nozione di trattamento anche le operazioni effettuate senza l'ausilio di strumenti elettronici, nonché quelle relative ad informazioni non organizzate in banche dati.

- **Titolare del Trattamento**: la persona fisica, la persona giuridica, la pubblica amministrazione o 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. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento l'entità nel suo complesso.
- **Responsabile del trattamento**: il Soggetto - persona fisica, persona giuridica, Pubblica Amministrazione o qualsiasi altro ente, associazione od organismo - preposto dal Titolare al trattamento di dati personali.
- **Responsabile Esterno del trattamento**: 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, ogni qualvolta il Titolare decida di affidare all'esterno dell'organizzazione un trattamento.
- **Incaricato**: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile.
- **Interessato**: il soggetto (persona fisica, persona giuridica, ente o associazione) cui si riferiscono i dati personali.
- **Garante per la Protezione dei dati personali**: organo collegiale che ha tra l'altro il compito di:
  - controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile;
  - esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati;
  - prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti;
  - vietare anche d ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco;
  - promuovere la sottoscrizione di codici deontologici;
  - esprimere pareri nei casi previsti.
- **AdS**: Amministratore di Sistema per come definito nel presente Regolamento;
- **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.

- **Agent**: programma o componente software capace di risolvere delle problematiche interagendo con altri software.
- **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**: (Amministratore di dominio) tipologia di amministratore di sistema con elevati livelli di autorizzazione (vedi ALLEGATO A al presente Regolamento). In caso di singolo dominio è equivalente all'Enterprise Administrator.
- **DPsS (o DPS)**: Documento Programmatico sulla Sicurezza; contiene la fotografia dello stato della sicurezza dell'organizzazione, 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 (vedi ALLEGATO A).
- **Export**: operazione di esportazione di dati o configurazioni da servizi o applicativi software.
- **Log**: (gergo nautico) pezzo di legno fissato ad una fune con nodi a distanza regolare lasciato galleggiare in mare, permette la misura approssimata della velocità della nave (da qui la misura convenzionale della velocità di una nave in nodi). (Informatica) registro cronologico degli eventi.
- **Logbook**: (gergo nautico) registro di navigazione dove annotare ad intervalli regolari velocità, meteo, forza del vento, oltre ad altri eventi significativi che si verificano durante la navigazione. (Informatica) documento di registrazione di tutti gli eventi (vedi Art. 11 del presente Regolamento).
- **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.
- **Registro degli incidenti alla sicurezza**: registro dove annotare tutti gli eventi avversi con risvolti (o possibili risvolti) su riservatezza, integrità e disponibilità delle informazioni.

- **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.
- **System Log**: registrazioni degli eventi di un singolo sistema.
- **System State**: salvataggio delle configurazione di un sistema.
- **Troubleshooting (lett. eliminazione del problema)**: processo di ricerca logica e sistematica delle cause di un problema.

Articolo 3 - Adempimenti previsti

Con il presente regolamento l'ASP di Crotone intende procedere ai seguenti adempimenti:

- individuare coloro che ricadono nella categoria di "AMMINISTRATORE DI SISTEMA";
- valutare l'esperienza, la capacità e l'affidabilità dei soggetti designati quali "AMMINISTRATORE DI SISTEMA" che devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento **ivi compreso il profilo relativo alla sicurezza**;
- designare tali "AMMINISTRATORE DI SISTEMA" in modo **individuale** con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato; l'incarico deve essere attribuito unicamente in via individuale e dunque non ad una società;
- verificare l'operato degli amministratori di sistema, con cadenza almeno annuale, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti
- **registrare gli accessi** ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema, mediante l'adozione di sistemi idonei alla registrazione degli accessi logici (autenticazione informatica).

Articolo 4 - Soggetti interessati

Soggetto interessato al presente regolamento è l'AMMINISTRATORE DI SISTEMA, quale figura professionale dedicata alla **gestione e alla manutenzione di impianti di elaborazione** *(compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza)* con cui vengano effettuati trattamenti di dati personali, e nella misura in cui consentano di intervenire sui dati personali.

Rientrano in questa accezione ampia di AMMINISTRATORE DI SISTEMA le figure chiamate a svolgere funzioni che comportano la concreta capacità di accedere, **in modo privilegiato**, a risorse del sistema informativo e a dati personali (anche qualora non siano preposte a operazioni che implicano una comprensione del dominio applicativo), e nella misura in cui sono, nelle loro consuete attività tecniche, responsabili di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali:

- salvataggio dei dati (backup/recovery);
- organizzazione dei flussi di rete;
- gestione dei supporti di memorizzazione;
- custodia delle credenziali di autenticazione e di autorizzazione;
- gestione dei sistemi di autenticazione e di autorizzazione;
- manutenzione hardware.

Possono dunque qualificarsi quale Amministratori di sistema i seguenti soggetti:

- amministratori di Sistemi di autenticazione;
- amministratori di server;
- amministratori di apparati rete;
- amministratori di base di dati;
- amministratori di apparati di sicurezza;
- amministratori di applicazioni.

Nell'ALLEGATO A al presente regolamento vengono riportate dettagliatamente le tipologie specifiche di Amministratore di Sistema, differenziate per livello di autorizzazione e profilo.

Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (per es. per scopi di manutenzione a seguito di guasti o malfunzionamenti) sui sistemi di elaborazione e sui sistemi software.

Articolo 5 - Elaborazione documento annuale Amministratori di Sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di **informazioni di carattere personale di lavoratori**, il TITOLARE e/o il RESPONSABILE è tenuto a rendere nota o conoscibile l'identità

degli amministratori di sistema, nell'ambito della propria organizzazione, attraverso la pubblicazione sul sito aziendale.

Nel caso di servizi di amministrazione di sistema affidati in **outsourcing** il TITOLARE e/o il RESPONSABILE del trattamento devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema dal Fornitore del servizio, in accordo con le prescrizioni di carattere generale da parte del Responsabile esterno del trattamento, preventivamente individuato.

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del TITOLARE e/o il RESPONSABILE del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

In esecuzione a quanto sopra, l'ASP di Crotone, su proposta dell'Ufficio Affari Generali Legali ed Assicurativi (l'Ufficio assicura tra l'altro anche le funzioni relative alla Gestione della Privacy) e l'U.O. Programmazione, Controllo di Gestione e Sistemi Informatici, delibera **annualmente** un documento contenente:

- l'elenco aggiornato degli amministratori di sistema, includente gli estremi identificativi degli amministratori di sistema e l'elenco delle funzioni loro attribuite;
- gli esiti della verifica della rispondenza dell'operato dell'AMMINISTRATORE DI SISTEMA alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Articolo 6 - Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. 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.

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 sei mesi.

Articolo 7 - Nomina dell'Amministratore di Sistema

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'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.

La designazione quale amministratore di sistema deve essere **in ogni caso individuale** e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

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 in materia di protezione dei dati personali, il TITOLARE o il RESPONSABILE devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei RESPONSABILI di cui all'art. 29 del Codice.

Il TITOLARE del TRATTAMENTO nomina "ENTERPRICE ADMINISTRATOR" il Dirigente dei Sistemi Informatici con atto scritto recante data certa (si veda il MODULO di cui all'ALLEGATO B al presente Regolamento).

La nomina di AMMINISTRATORE di SISTEMA, su indicazione del Direttore del Distretto, Dipartimento e/o Unità Operativa Complessa, avviene a cura del ENTERPRICE ADMINISTRATOR, ed è effettuata anch'essa con atto scritto recante data certa (si veda il MODULO di cui all'ALLEGATO C al presente Regolamento), contenente per lo meno:

- gli "estremi identificativi" dell'Amministratori di Sistema (si tratta del minimo insieme di dati identificativi utili a individuare il soggetto nell'ambito dell'organizzazione di appartenenza: nome, cognome, funzione o area organizzativa di appartenenza etc. etc.);
- elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Tutti gli atti di nomina dovranno essere controfirmati dall'Incaricato per accettazione.

L'*Enterprise Administrator* (vedi ALLEGATO A) crea l'account personale dell'Amministratore di Sistema nominato ed associa il profilo minimo necessario secondo quanto stabilito dal Dirigente dei Sistemi Informatici. La password deve essere inserita nel sistema di gestione dell'autenticazione direttamente dalla persona fisica nominata o in alternativa, il sistema

genera una password che comunica direttamente ed in modalità sicura sempre alla persona fisica nominata.

Articolo 8 - Funzioni e compiti dell'Amministratore di Sistema

Le FUNZIONI dell'Amministratore di Sistema si differenziano in base alla tipologia specifica di Amministratore ed al profilo di autorizzazione (si veda l'ALLEGATO A al presente regolamento).

In via del tutto generale l'AdS è chiamato a svolgere le funzioni richiamate nel "*Disciplinare tecnico in materia di misure minime di sicurezza*", di cui all'ALLEGATO B al D.lgs. n.ro 196/2003 (Artt. da 33 a 36 del Codice) e, più in generale, che comportano la concreta capacità di accedere, in modo privilegiato, a risorse del sistema informativo e a dati personali (anche qualora non siano preposte a operazioni che implicano una comprensione del dominio applicativo), e nella misura in cui sono, nelle loro consuete attività tecniche, responsabili di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali:

- realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati);
- organizzazione dei flussi di rete;
- gestione dei supporti di memorizzazione;
- custodia delle credenziali di autenticazione e di autorizzazione;
- gestione dei sistemi di autenticazione e di autorizzazione;
- manutenzione hardware.

L'AMMINISTRATORE DI SISTEMA inoltre:

- ☐ tratta i dati personali in modo lecito e secondo correttezza ed esclusivamente per gli scopi inerenti l'attività svolta nell'ambito delle proprie mansioni;
- ☐ verifica, ove possibile, che tali dati siano esatti e, se lecito e necessario, li aggiorna;
- ☐ verifica che tali dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati;
- ☐ tratta tali dati rispettando le misure di sicurezza previste dalla normativa in materia di privacy e in particolare dalle indicazioni previste dall'Allegato B al Codice;
- ☐ informare il RESPONSABILE del trattamento o il TITOLARE in caso di mancato rispetto alle norme di sicurezza e in caso di eventuali incidenti;
- ☐ non utilizza a fini privati i dati cui accede;
- ☐ non consente a terzi non legittimati l'accesso ai dati ottenuti in ragione dell'espletamento dei propri compiti;
- ☐ non divulga eventuali dati riservati di cui venisse a conoscenza;
- ☐ non interferisce illegittimamente nel lavoro altrui;

- non altera illegittimamente o danneggia i dati cui accede;
- non effettua controlli illegittimi sulla attività degli utenti del sistema;

A causa della indifferenziata possibilità di accesso ai dati ed i conseguenti rischi per la riservatezza dei soggetti interessati, l'AMMINISTRATORE DI SISTEMA utilizza le relative funzioni e privilegi solo quando necessario o indispensabile.

Il Direttore Amministrativo
Dott. Giuseppe FICO

Il Direttore Generale f.f.
Dott. Agostino TALERICO

REGOLAMENTO CONCERNENTE LA NOMINA, LE FUNZIONI ED I COMPITI DEGLI AMMINISTRATORI DI SISTEMA DELL'ASP di CROTONE adottato con DELIBERA N. 090 DEL 04 AGO. 2017

ALLEGATO A - Tipologia di Amministratore e profili di autorizzazione

Enterprise Administrator

RUOLO
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.

PROFILO di AUTORIZZAZIONE
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

RUOLO
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.

PROFILO di AUTORIZZAZIONE
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. 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

RUOLO
Amministratore di un singolo sistema server.

PROFILO di AUTORIZZAZIONE
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
RUOLO Amministratore degli *account* utente per il solo dominio di appartenenza. **PROFILO di AUTORIZZAZIONE** Autorizzato: 1. alla creazione/disabilitazione degli *account utente*; 2. all'assegnazione del profilo di autorizzazione all'*account utente*.

Network Administrator
RUOLO Amministratore dell'infrastruttura di rete e di comunicazione. **PROFILO di AUTORIZZAZIONE** 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
RUOLO Amministratore dei dispositivi di sicurezza **PROFILO di AUTORIZZAZIONE** 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
RUOLO Amministratore di un database server o di una singola istanza di database **PROFILO di AUTORIZZAZIONE** 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
RUOLO Amministratore dei backup e delle repliche dei dati **PROFILO di AUTORIZZAZIONE** 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
RUOLO Amministratore di un singolo servizio o applicazione (es. mail server, web server, application server) **PROFILO di AUTORIZZAZIONE** 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
RUOLO Amministratore locale di singoli sistemi *client* **PROFILO di AUTORIZZAZIONE** 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.

REGOLAMENTO CONCERNENTE LA NOMINA, LE FUNZIONI ED I COMPITI DEGLI AMMINISTRATORI DI SISTEMA DELL'ASP di CROTONE adottato con DELIBERA N. 090 DEL 04 AGO.2017

ALLEGATO B - Atto di nomina di ENTERPRICE ADMINISTRATOR

Egr. Sig./Dott. _____

OGGETTO: Nomina dell'Amministratore di Sistema in applicazione del "Codice in materia di protezione dei dati personali" di cui al D.Lgs. n. 196/2003 e ss.mm.ii.

L'ASP di Crotone in qualità di TITOLARE del trattamento dei dati personali effettuati anche con strumenti elettronici, ai sensi dell'articolo 28 del D.Lgs. n.196/2003 e ss.mm.ii. recante "Codice in materia di protezione dei dati personali";

DATO il Rapporto di Lavoro con Lei in essere; VISTO l'incarico di Dirigente dei Sistemi Informatici/Responsabile IT (Information Technologies) a Lei conferito da questa Azienda;

CONSIDERATO
- CHE si ritiene che la S.V. sia Soggetto idoneo ad assurgere a ruolo di ENTERPRICE ADMINISTRATOR, essendo in possesso di tutte le caratteristiche di esperienza, capacità e affidabilità necessarie per adempiere agli obblighi in materia di sicurezza del trattamento informatico dei dati;
- CHE le prestazioni da lei effettuate in via ordinaria forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;

VISTO il Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e ss.mm.ii. ed in particolare, l'allegato B) al predetto Decreto "*Disciplinare tecnico in materia di misure minime di sicurezza*";

VISTO il Provvedimento del Garante della Privacy del 27 Novembre 2008 recante "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", così come modificato dal Provvedimento del 25 giugno 2009;

CON LA PRESENTE NOMINA LA S.V.
ENTERPRICE ADMINISTRATOR

con il seguente PROFILO di AUTORIZZAZIONE
1. autorizzato 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. autorizzato alla creazione degli account ed abilitazione degli accessi agli Administrator di livello 0, 1 e 2 di tutti i domini;
3. autorizzato all'analisi e controllo dei log di tutte le macchine appartenenti a tutti i domini e dei dispositivi di tutta la rete.

Si precisa che in via del tutto generale l'AdS è chiamato a svolgere le funzioni richiamate nel "*Disciplinare tecnico in materia di misure minime di sicurezza*", di cui all'ALLEGATO B al D.lgs. n.ro 196/2003 e ss.mm.ii. (Artt. da 33 a 36 del Codice) e, più in generale, che comportano la concreta capacità di accedere, in modo privilegiato, a risorse del sistema informativo e a dati personali (anche qualora non siano preposte a operazioni che implicano una comprensione del dominio applicativo), e nella misura in cui sono, nelle loro consuete attività tecniche, responsabili di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali:

- realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati);
- organizzazione dei flussi di rete;
- gestione dei supporti di memorizzazione;
- custodia delle credenziali di autenticazione e di autorizzazione;
- gestione dei sistemi di autenticazione e di autorizzazione;
- manutenzione hardware.

A causa della indifferenziata possibilità di accesso ai dati ed i conseguenti rischi per la riservatezza dei soggetti interessati, l'AMMINISTRATORE DI SISTEMA utilizza le relative funzioni e privilegi solo quando necessario o indispensabile.

L'operato degli Amministratori di Sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del TITOLARE e/o il RESPONSABILE del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

IL TITOLARE del TRATTAMENTO
Il Direttore Generale ASP di Crotone

_____

Crotone lì,_____

Per accettazione:
L'ENTERPRICE ADMINISTRATOR

_____

REGOLAMENTO CONCERNENTE LA NOMINA, LE FUNZIONI ED I COMPITI DEGLI AMMINISTRATORI DI SISTEMA DELL'ASP di CROTONE adottato con DELIBERA N. 090 DEL 04 AGO.2017

ALLEGATO C - Atto di nomina di Amministratore di Sistema

Egr. Sig./Dott. _____

OGGETTO: Nomina dell'Amministratore di Sistema in applicazione del "Codice in materia di protezione dei dati personali" di cui al D.Lgs. n. 196/2003 e ss.mm.ii.

L'ASP di Crotone in qualità di TITOLARE del trattamento dei dati personali effettuati anche con strumenti elettronici, ai sensi dell'articolo 28 del D.Lgs. n.196/2003 e ss.mm.ii. recante "Codice in materia di protezione dei dati personali";

PREMESSO che con lettera prot. n.ro _____ del _____

- ☐ il Direttore del Distretto_____
- ☐ il Direttore del Dipartimento_____
- ☐ il Direttore dell'Unità Operativa Complessa_____

ha indicato la S.V. quale Soggetto idoneo ad assurgere a ruolo di Amministratore di Sistema, essendo in possesso di tutte le caratteristiche di esperienza, capacità e affidabilità necessarie per adempiere agli obblighi in materia di sicurezza del trattamento informatico dei dati;

CONSIDERATO che le prestazioni da lei effettuate in via ordinaria forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;

VISTO il Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e ss.mm.ii. ed in particolare, l'allegato B) al predetto Decreto "*Disciplinare tecnico in materia di misure minime di sicurezza*";

VISTO il Provvedimento del Garante della Privacy del 27 Novembre 2008 recante "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", così come modificato dal Provvedimento del 25 giugno 2009;

CON LA PRESENTE NOMINA LA S.V.
AMMINISTRATORE DI SISTEMA (AdS)

Con le seguenti funzioni *(specificare tipologia di Amministratore e profili di autorizzazione di cui all'ALLEGATO A al Regolamento):*

Si precisa che in via del tutto generale l'AdS è chiamato a svolgere le funzioni richiamate nel "*Disciplinare tecnico in materia di misure minime di sicurezza*", di cui all'ALLEGATO B al D.lgs. n.ro 196/2003 e ss.mm.ii. (Artt. da 33 a 36 del Codice) e, più in generale, che comportano la concreta capacità di accedere, in modo privilegiato, a risorse del sistema informativo e a dati personali (anche qualora non siano preposte a operazioni che implicano una comprensione del dominio applicativo), e nella misura in cui sono, nelle loro consuete attività tecniche, responsabili di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali:

- realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati);
- organizzazione dei flussi di rete;
- gestione dei supporti di memorizzazione;
- custodia delle credenziali di autenticazione e di autorizzazione;
- gestione dei sistemi di autenticazione e di autorizzazione;
- manutenzione hardware.

L'AMMINISTRATORE DI SISTEMA inoltre:

- ☐ tratta i dati personali in modo lecito e secondo correttezza ed esclusivamente per gli scopi inerenti l'attività svolta nell'ambito delle proprie mansioni;
- ☐ verifica, ove possibile, che tali dati siano esatti e, se lecito e necessario, li aggiorna;
- ☐ verifica che tali dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati;
- ☐ tratta tali dati rispettando le misure di sicurezza previste dalla normativa in materia di privacy e in particolare dalle indicazioni previste dall'Allegato B al Codice;
- ☐ informare il RESPONSABILE del trattamento o il TITOLARE in caso di mancato rispetto alle norme di sicurezza e in caso di eventuali incidenti;
- ☐ non utilizza a fini privati i dati cui accede;
- ☐ non consente a terzi non legittimati l'accesso ai dati ottenuti in ragione dell'espletamento dei propri compiti;
- ☐ non divulga eventuali dati riservati di cui venisse a conoscenza;
- ☐ non interferisce illegittimamente nel lavoro altrui;
- ☐ non altera illegittimamente o danneggia i dati cui accede;
- ☐ non effettua controlli illegittimi sulla attività degli utenti del sistema;

Gli ambiti di operatività consentiti in base al Suo profilo di autorizzazione (cioè i trattamenti dei dati a Lei consentiti) sono:

A causa della indifferenziata possibilità di accesso ai dati ed i conseguenti rischi per la riservatezza dei soggetti interessati, l'AMMINISTRATORE DI SISTEMA utilizza le relative funzioni e privilegi solo quando necessario o indispensabile.

L'operato degli Amministratori di Sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del TITOLARE e/o il RESPONSABILE del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

L'ENTERPRICE ADMINISTRATOR

_____

Crotone lì,_____

Per accettazione:
L'Amministratore di Sistema

Dott. _____