SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Imola

FRONTESPIZIO DELIBERAZIONE

AOO: AS_BO66

REGISTRO: Deliberazione

NUMERO: 0000135

DATA: 30/07/2024 10:09

OGGETTO: PROVVEDIMENTI IN MERITO ALLA DESIGNAZIONE DEGLI AMMINISTRATORI DI SISTEMA IN ATTUAZIONE DELLE INDICAZIONI DELL' AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Rossi Andrea in qualità di Direttore Generale
Con il parere favorevole di Neri Andrea - Direttore Sanitario
Con il parere favorevole di Donattini Maria Teresa - Direttore Amministrativo

Su proposta di Cristian Chiarini - TECNOLOGIE SANITARIE E INFORMATICHE SANITARIE E DI RETE che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [07-05-01]

DESTINATARI:

- Collegio sindacale
- TECNOLOGIE SANITARIE E INFORMATICHE SANITARIE E DI RETE
- DIREZIONE GENERALE
- DIREZIONE MEDICA DI PRESIDIO
- DIPARTIMENTO CURE PRIMARIE
- DIPARTIMENTO SALUTE MENTALE
- DIPARTIMENTO DI SANITA' PUBBLICA
- INFORMAZIONE E COMUNICAZIONE
- FORMAZIONE
- DISTRETTO

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000135_2024_delibera_firmata.pdf	Chiarini Cristian; Donattini Maria Teresa; Neri Andrea; Rossi Andrea	80A1318324ED7FF6FAFEF4219DE087E32E9A97ABB53CFDE61205C9355E37111C

File	Firmato digitalmente da	Hash
DELI0000135_2024_Allegato1.pdf:		A142768D948A93233BD6CDEAC96D6864 FD5D52AEB1479555677E934E7AD2D7CF
DELI0000135_2024_Allegato2.pdf:		74794A2249B513241528E645DC730BF75 23504168A9B3C3B24B671AD241C2CC2

DELIBERAZIONE

OGGETTO: PROVVEDIMENTI IN MERITO ALLA DESIGNAZIONE DEGLI AMMINISTRATORI DI SISTEMA IN ATTUAZIONE DELLE INDICAZIONI DELL'AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

IL DIRETTORE GENERALE

Su proposta del Direttore della UOC Tecnologie Sanitarie, Informatiche Sanitarie e di Rete che esprime contestuale parere favorevole in ordine ai contenuti formali sostanziali e di legittimità del presente atto;
Richiamati:

il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR);

il Decreto Legislativo n. 101 del 10 agosto 2018, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679;

la deliberazione n. 158 del 15/12/2009, avente ad oggetto "Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (e succ. mod.) Amministratori di sistema. Attuazione delle prescrizioni";

la deliberazione n. 57 del 06/03/2023, avente ad oggetto "Aggiornamento del documento "Linee guida per l'applicazione del Regolamento UE 2016/679 e del D.Lgs. 30.06.2003 n. 196"";

la deliberazione n. 136 del 15/06/2022, avente ad oggetto "Approvazione disciplinare aziendale sull'utilizzo della posta elettronica e di internet";
Visti:

- il Provvedimento dell'Autorità Garante per la protezione dei dati personali 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*";
- il Provvedimento dell'Autorità Garante per la protezione dei dati personali del 25 giugno 2009 recante " *Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento"*;
- la disposizione transitoria e finale del D.lgs. 101/2018, art. 22, comma 4, per la quale " *a decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto";*

Atteso che l'Autorità Garante definisce quali amministratori di sistema " *Le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (quali ad esempio gli amministratori di dominio e di server), nonché le 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*" prescrivendo in particolare:

1. che l'attribuzione delle funzioni di amministratore di sistema debba avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza;
2. che la designazione quale amministratore di sistema debba essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
3. la divulgazione dell'identità e delle mansioni degli amministratori di sistema al personale, qualora l'attività di costoro possa entrare in contatto con dati personali dei dipendenti, anche in considerazione dei possibili impatti con le garanzie previste dallo statuto dei lavoratori in tema di controllo;
4. che il tracciamento dei log degli accessi degli amministratori di sistema sia da conservare per sei mesi e la vigilanza dell'operato degli amministratori di sistema è attribuita al Direttore dell'UOC Tecnologie Sanitarie, Informatiche Sanitarie e di Rete, come parimenti indicato all'interno della Politica di gestione degli Amministratori di Sistema (ADS);
5. che, nel caso di servizi di amministratore di sistema affidati in outsourcing, il titolare o il responsabile del trattamento debba conservare direttamente e specificatamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;

Considerata la necessità per l'Azienda USL di definire ed adottare gli indirizzi per assicurare la conformità dell'operato degli Amministratori di Sistema alle prescrizioni dei sopra richiamati Provvedimenti dell'Autorità Garante e, in particolare, porre in essere adempimenti per la designazione individuale degli stessi con elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

Dato atto che il Responsabile Protezione Dati (DPO) ha attivato apposito gruppo di lavoro per definire in ambito metropolitano modalità omogenee di designazione degli amministratori di sistema e che, a conclusione dei lavori, ha trasmesso il fac simile di atto di designazione, allegato quale parte integrante al presente provvedimento;

Ritenuto pertanto di recepire l'allegato fac simile di atto di designazione individuale degli amministratori di sistema interni all'Azienda USL di Imola, dando mandato al Direttore dell'UOC Tecnologie Sanitarie,

Informatiche Sanitarie e di Rete, previo coordinamento con il Responsabile della UO alla quale appartiene l' amministratore di sistema interno all'Azienda, di proporre al Direttore Generale l'elenco nominativo degli amministratori di sistema interni all'Azienda da nominare.

Delibera

1. Di approvare l'aggiornamento del documento "Disciplinare ADS. Politica di gestione degli Amministratori di Sistema" allegato alla presente deliberazione quale parte integrante e sostanziale;
2. Di adottare lo schema tipo dell'atto di designazione alle funzioni di Amministratore di sistema elaborato dall'apposito gruppo di lavoro coordinato dal DPO e da quest'ultimo trasmesso alle Aziende Sanitarie dell'area Metropolitana per la conseguente adozione;
3. Di demandare al Direttore dell'UOC Tecnologie Sanitarie, Informatiche Sanitarie e di Rete, previo coordinamento con il Responsabile della UO alla quale appartiene l'amministratore di sistema interno all'Azienda, di proporre al Direttore Generale, in qualità di Titolare, gli amministratori di sistema interni all'Azienda da nominare mediante il suddetto schema.
4. Di demandare altresì al medesimo Direttore della UOC Tecnologie Sanitarie, Informatiche Sanitarie e di Rete la tenuta dell'elenco aggiornato degli Amministratori di sistema in ottemperanza alle disposizioni dell'Autorità Garante Privacy;
5. Di individuare quale responsabile del procedimento ai sensi della Legge n. 241/90 l'Ing. Cristian Chiarini;
6. Di trasmettere copia della presente deliberazione al Collegio Sindacale, ai sensi dell'art. 18, comma 4, della L.R. 16.7.2018 n. 9.

Prot.

Oggetto: Designazione ad "Amministratore di sistema"

Al/Alla Sig. /Sig.ra _____ nato/a a _____ il _____,

matricola _____ qualifica _____

UO _____ sede _____

Premesso che,

- nell'ambito della propria attività l'Ausl di Imola, in qualità di Titolare del trattamento, tratta dati personali, compreso dati personali di natura particolare, avvalendosi anche di strumenti elettronici;
- tali trattamenti sono soggetti alle disposizioni del Regolamento (UE) 2016/679 (GDPR), della normativa italiana di armonizzazione (D.lgs. 30 giugno 2003, n.196 s.m.i. recante il "Codice in materia di protezione dei dati personali"), nonché ai Provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali;
- in forza del Provvedimento a carattere generale del 27 novembre 2008, "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, l'Autorità Garante ha prescritto per i soggetti pubblici e privati l'adeguamento delle misure di sicurezza già in uso con l'adozione di altre e ulteriori finalizzate al corretto svolgimento delle funzioni degli Amministratori di sistema;
- l'attribuzione delle funzioni di Amministratore di sistema deve avvenire, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, secondo le prescrizioni dell'Autorità Garante per la Protezione dei Dati Personali.

Preso atto che, così come definito dai richiamati provvedimenti dell'Autorità, l'Amministratore di Sistema è:

- *"una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali";*
- *"…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.".*

Preso atto, inoltre, che non rientrano nelle definizioni su elencate quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzionamenti) sui sistemi di elaborazione e sui sistemi software, così come chiarito nella FAQ n. 1 al Provvedimento del 27 novembre 2008 dell'Autorità Garante per la Protezione dei Dati Personali sopra richiamato[1].

[1] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1577499#FAQ

CON LA PRESENTE

ad integrazione della nomina quale "Persona autorizzata al trattamento dei dati personali", avendo valutato che le prestazioni da Lei effettuate in via ordinaria forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza, la S.V. è designata quale "Amministratore di sistema".

Per effetto di tale designazione e delle funzioni conseguentemente attribuite, Lei si impegna a:

- accedere ai sistemi ICT nei limiti strettamente richiesti dall'espletamento delle Sue mansioni;
- eseguire gli accessi nel rispetto delle procedure di autenticazione a Lei già note, e di detenzione, custodia, segretezza e sicurezza delle relative credenziali di accesso;
- eseguire gli accessi nel rispetto delle misure di sicurezza organizzative, logiche e fisiche adottate dal Titolare del trattamento;
- attenersi alle istruzioni operative impartite dal Direttore/Responsabile della UO di appartenenza e dal servizio UOC Tecnologie Sanitarie, Informatiche Sanitarie e di Rete;
- segnalare qualunque elemento che possa pregiudicare il corretto svolgimento delle Sue funzioni di Amministratore di sistema e/o rendere necessarie ulteriori istruzioni;
- cooperare con il Direttore/Responsabile della UO di appartenenza e con il servizio UOC Tecnologie Sanitarie, Informatiche Sanitarie e di Rete per ogni verifica della rispondenza del Suo operato alle misure organizzative, tecniche e di sicurezza previste con riferimento ai dati personali trattati per conto e nell'interesse dell'Ente;
- collaborare per l'attuazione delle eventuali ulteriori prescrizioni che saranno emanate dall'Autorità Garante per la Protezione dei Dati Personali in tema di Amministratori di sistema;
- consentire il trattamento dei Suoi dati personali nei limiti e per le finalità previste dal citato Provvedimento del 27 novembre 2008 dell'Autorità Garante per la Protezione dei Dati Personali, incluse la registrazione e comunicazione di ogni dato di log relativo all'attività di Amministratore di sistema.

Nello specifico l'incarico è rappresentato dal seguente profilo

Profilo:

☐ Sistemisti S.O.

☐ Amministratori di rete

☐ Amministratori di database

☐ Sistemisti gestori applicativi

Ampiezza: *Server, DB e applicativi area sanitaria*

come riportati nel documento "Politica di gestione degli Amministratori di Sistema" allegato alla presente e pubblicato nell'intranet aziendale, alla sezione Privacy.

Resta inteso e convenuto che:

- la presente designazione non configura alcuna variazione della Sua qualifica e delle Sue mansioni e del relativo trattamento economico e normativo del rapporto di lavoro con Lei in essere;
- la registrazione e comunicazione dei dati di log sarà eseguita al solo fine di ottemperare a quanto specificatamente prescritto al riguardo dal su citato Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali e non costituisce alcuna forma di controllo a distanza, neanche indiretto, della Sua attività lavorativa;
- ogni eventuale variazione dell'ambito di operatività consentito dalle Sue mansioni e dal Suo profilo di autorizzazione all'accesso ai sistemi ICT non comporterà il venir meno degli effetti della presente designazione.

Si rammenta, inoltre, che il Provvedimento del Garante già citato, obbliga il Titolare del trattamento alla verifica almeno annuale delle attività svolte dall'Amministratore di sistema, in modo da controllare la rispondenza di tali attività alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Il Direttore Generale

_____

Letto firmato e sottoscritto per accettazione

L'Amministratore di sistema

_____

Data

_____

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Imola

Politica di gestione degli Amministratori di Sistema (ADS)

2024

Disciplinare ADS

Versione/stato	Data	Autore	Sintesi
1.0/bozza	02/11/2009	Darchini	Prima stesura
1.1/bozza	29/11/2009	Darchini	Inserito parte tecnologica (progettata da ditta VEM sistemi. Revisionato a seguito confronto con gruppo privacy aziendale e con avv. Sandra Reggio
1.2 /definitivo	10/12/2009	Darchini	Revisionato a seguito confronto dott. Fiorentini e con dott. Sandra Reggio
1.3/definitivo	15/07/2024	Nanni	Revisionato a seguito di aggiornamento normativo ex Reg. (UE) 2016/679 (cd. GDPR) e ai sensi del D. Lgs. 196/2003 come novellato dal D.Lgs. 101/2018. Revisionato a seguito dell'istituzione del Gruppo di Lavoro sugli Amministratori di sistema, coordinato dal Data Protection Officer aziendale.

Sommario

1. Introduzione ed obiettivi

Il Provvedimento a carattere generale adottato in data 27 novembre 2008 dall'Autorità Garante per la protezione dei dati personali, prescrive ai titolari di trattamenti effettuati con strumenti elettronici una serie di misure a carattere tecnico ed organizzativo volte a controllare e contenere i rischi e le criticità implicite allo svolgimento dell'incarico da parte delle persone preposte alla mansione di Amministratore di Sistema.

Il summenzionato provvedimento è stato successivamente oggetto di modifiche da parte del Garante stesso con il provvedimento del 25 giugno 2009 "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento" (G.U. n. 149 del 30 giugno 2009).

Attraverso l'adozione di tali misure l'organizzazione può attuare un processo di gestione controllato in ordine all'operato di tali figure, le quali tipicamente dispongono di profili di autenticazione che consentono un accesso privilegiato alle risorse del sistema informativo che può comportare concretamente accessi a dati personali che vanno oltre la legittimazione attribuita.

Con l'entrata in vigore del Regolamento europeo n. 2016/679 (cd. GDPR) e del D.Lgs. n. 101/2018 che ha novellato il D. Lgs. n. 196/2003 (cd. Codice), sono state introdotte ulteriori prescrizioni sulle misure a carattere tecnico ed organizzativo che ciascuna organizzazione deve adottare al fine di garantire e dimostrare che le operazioni di trattamento vengano effettuate in conformità ai principi fondamentali della disciplina in materia (cfr. artt. 24, 25, 29, 32, 35 e 36 del GDPR).

Tali prescrizioni sono applicabili altresì ai Responsabili esterni del trattamento, nominati dal Titolare, ai sensi del GDPR e, in particolar modo, ai sensi dell'art. 28 del GDPR.

Il presente documento si pone l'obiettivo di descrivere le misure organizzative adottate dall'Ente al fine di dare esecutività al provvedimento, alla luce degli aggiornamenti normativi summenzionati (GDPR e Codice), tenuto conto altresì delle disposizioni di cui alla Circolare n. 2/2017 AgID "Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015)".

L'Azienda USL di Imola ha sempre colto come opportunità le sollecitazioni di volta in volta proposte da disposti normativi e/o provvedimenti del Garante in materia di sicurezza.

Il sistema informativo di una azienda sanitaria ha caratteristiche, per dimensioni e contenuti, assolutamente rilevanti e, come tale, richiede la migliore gestione possibile soprattutto per quanto riguarda la sicurezza.

L'applicazione di quanto previsto dalle norme rappresenta per l'Azienda, ovvero per le sue strutture operative, uno strumento attraverso il quale l'organizzazione ha modo di standardizzare processi e regolamentare l'utilizzo delle tecnologie.

Sono stati inoltre adottati con delibera n. 136/2022 il "Disciplinare aziendale sull'utilizzo della posta elettronica e di internet" e con delibera n. 41/2021 il "Disciplinare tecnico in materia di videosorveglianza", entrambi volti a disciplinare l'utilizzo di strumenti informatici e tecnologie in uso in Azienda e a garantire la riservatezza dei dati trattati con tali strumenti/dispositivi.

Nel caso in cui il servizio, e il ruolo, di amministratore di sistema sia affidato in outsourcing (v. infra § 2 "Profili professionali e ambiti di operatività"), la ricognizione dei trattamenti dei dati e delle relative nomine delle Ditte esterne in qualità di Responsabili del trattamento è effettuata annualmente, in conformità alle disposizioni di cui alla delibera n. 57 del 06/03/2023.

2. Profili professionali e ambiti di operatività

L'Azienda USL di Imola ha ritenuto di individuare quali amministratori di sistema tutti gli operatori dell'Azienda (dipendenti) che operano sui sistemi informatici aziendali per attività di:

- network administration
- data base administration
- system administration

ovvero, più in generale, operatori che interagiscono con banche dati contenenti dati personali e sensibili senza l'intermediazione di software applicativi ma mediante linguaggi di inquiry (sql).

I diversi profili di amministratore di sistema sono stati individuati sulla base delle seguenti caratteristiche:

- livello di autonomia tecnologica; si intende la possibilità di agire sui sistemi gestiti (server, db, reti, client…) attraverso strumenti tecnologici più o meno potenti e/o flessibili, (a titolo di esempio: con l'accesso ai dati mediante un applicativo si possono effettuare solo le operazioni previste dall'applicativo e le operazioni effettuate sono di norma tracciate, viceversa chi accede a un database mediante query SQL ha la possibilità di effettuare operazioni di qualunque genere su qualunque tabella);
- potenziale visibilità dei dati; si intende il grado di "vicinanza" dell'amministratore con i dati, l'amministratore di database o il gestore applicativo ha una elevata vicinanza al dato, viceversa il sistemista di sistemi operativi o l'amministratore di rete non ha diretta visibilità dei dati;
- rischio potenziale governato; si intende appunto la dimensione del rischio a cui espone l'azienda un errato o doloso comportamento da parte dell'amministratore di sistema. Sono parametri di misurazione la numerosità degli utenti che potrebbero risentire di eventuali malfunzioni derivanti da errati o dolosi comportamenti dell'ADS nonché la consistenza delle banche dati.

Si individuano di conseguenza le seguenti figure specifiche di amministratore di sistema:

- **sistemisti S.O.**
- **amministratori di rete**
- **amministratori di database**
- **sistemisti gestori applicativi**

La presente politica si applica pertanto agli operatori dell'Azienda (dipendenti) che ricoprono il ruolo di Amministratori di sistema, come sopra definito, e in conformità all'atto di designazione.

Il ruolo di Amministratore di sistema può essere ricoperto da soggetti non dipendenti dell'Azienda (cd. ADS outsourcer); in tal caso il servizio di amministratore di sistema viene regolato mediante la stipula di contratti o trasmissione di ordini, entrambi effettuati dal Servizio gestore del contratto/ordine o dal Settore Dipartimento Amministrativo Tecnico (U.O. Economato e Logistica).
In particolar modo, la Ditta viene nominata quale Responsabile del trattamento dei dati; tale nomina include e disciplina gli adempimenti ai quali sono tenuti gli incaricati della Ditta in qualità di amministratori di sistema.

Ai sensi dei sopra citati provvedimenti del Garante, non rientrano nella definizione di "Amministratore di sistema" quei soggetti che solo occasionalmente intervengono (ad esempio, per scopi di manutenzione a seguito di guasti o malfunzionamenti) sui sistemi di elaborazione e sui sistemi software.
Sono altresì esclusi dall'ambito di applicazione i servizi svolti per ordinarie finalità amministrativo-contabili.

3. Modalità per l'esercizio delle funzioni di Amministratore di sistema

È specifico compito dell'Amministratore di sistema, come sopra definito, attivarsi per tutelare, nei limiti delle proprie competenze e capacità professionali, la protezione dei dati, il buon funzionamento dei sistemi e la continuità operativa dei medesimi. In generale l'Amministratore di sistema, limitatamente al profilo ed all'ampiezza del ruolo assegnati attraverso apposita lettera di designazione, è tenuto a:

- sovrintendere alle risorse di sistema operativo ed alle basi di dati in modo tale da garantire l'efficienza del sistema tecnologico e l'aderenza delle configurazioni ai profili di autorizzazione stabiliti per i soggetti autorizzati al trattamento dati;
- vigilare sul corretto uso dei sistemi da parte dei tecnici che operano, a vario titolo, sul sistema e sulle sue componenti periferiche e da parte degli altri incaricati, segnalando eventuali usi scorretti o impropri;
- assegnare e gestire gli identificativi di utente (UserId) in modo che siano univoci sul sistema e quindi adeguati ad identificare anagraficamente l'operatore che accede ed opera sul sistema;
- rilasciare la prima password agli utenti ed assicurarsi che gli utenti ricevano le istruzioni operative per il corretto utilizzo dei sistemi;
- predisporre meccanismi di protezione da accessi indesiderati e meccanismi di protezione nei confronti di attacchi da virus: tali meccanismi sono periodicamente aggiornati e verificati;
- mantenere i sistemi allineati con la reale situazione degli utenti e con i loro profili di autorizzazione;
- supportare la gestione sicura dei supporti di memoria, interni o esterni al sistema di trattamento provvedendo a che le informazioni in essi contenute siano conservate e custodite in modo sicuro, non siano accessibili ad estranei ed eventualmente provvedere alla loro distruzione;
- evitare, ove non strettamente indispensabile per lo svolgimento delle operazioni tecniche connesse al proprio ruolo, di entrare in contatto, visualizzare, maneggiare o mettere a rischio dati personali;
- segnalare al proprio Responsabile la necessità di aggiornamento professionale per garantire uno svolgimento del proprio ruolo in linea con il progresso tecnologico.

Gli Amministratori di sistema sono responsabili dei sistemi sui quali operano pertanto devono agire con attenzione, cautela, consapevolezza delle proprie azioni e delle conseguenze relative derivabili da imperizia, disattenzione e incauta gestione del sistema. L'incarico di Amministratore di sistema è assegnato sulla base di una riconosciuta capacità professionale, di una specifica competenza in materia e di un percorso professionale definito (cfr. § 3.1 Valutazione delle caratteristiche soggettive).

Per ciascuna figura si riportano di seguito le mansioni attribuite e conseguentemente gli ambiti di attività. In generale gli ADS hanno titolo all'utilizzo delle credenziali assegnate esclusivamente nell'ambito delle mansioni assegnate e secondo quanto definito nello specifico atto di designazione.

3.1 Sistemisti S.O. (ADS – SO)

Gli Amministratori di Sistema con profilo di autorizzazione di sistemista Sistemi Operativi sono autorizzati ad operare su tutti i sistemi operativi server e sono tenuti a svolgere le seguenti attività:

- sorvegliare il corretto funzionamento dei sistemi in senso generale (monitoraggio) e dei sottosistemi specifici in particolare (CPU, memorie, sistemi dischi, storage, schede di rete, sistema di alimentazione e di ventilazione, ecc.);
- sorvegliare il corretto funzionamento dei sistemi applicativi a bordo della piattaforma tramite il monitoraggio dei log e dei messaggi prodotti dal sistema operativo e dal software di base;
- intervenire ogni qualvolta venga evidenziato un malfunzionamento, un guasto o una anomalia funzionale sui sistemi, sui servizi erogati tramite la piattaforma, per diagnosticare il problema e ripristinare il corretto funzionamento dei sistemi;
- intervenire periodicamente per verificare e, compatibilmente con i vincoli introdotti dai sistemi applicativi ospiti, aggiornare il sistema operativo, i driver di periferiche, ed ogni componente del software di base per garantire l'allineamento della piattaforma con le versioni emesse dal produttore / costruttore;
- provvedere alla configurazione ottimale del sistema per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità/onerosità di gestione e mantenimento nel tempo delle funzioni;
- intervenire prontamente in situazioni di emergenza o in caso di manutenzione ordinaria o straordinaria per segnalare i bisogni dell'organizzazione ai fornitori esterni dell'assistenza tecnica, coordinare e seguire gli interventi relativi, informare gli utenti e le strutture tecniche coinvolte;
- segnalare eventuali problematiche dei sistemi o situazioni anomale ai dirigenti della UO Tecnologie Sanitarie, Informatiche Sanitarie e di Rete;
- definire e configurare gli utenti, gli account che devono operare sul sistema ed i parametri relativi, attribuendo loro il profilo di autorizzazione indicato dal Responsabile del trattamento cui il sistema è di supporto;
- cooperare all'installazione dei sistemi, monitorare la loro continuità operativa e la fruibilità continuativa dei servizi da parte degli utenti, verificare la funzionalità delle interfacce e attivare e disattivare i singoli processi software per garantire detta continuità di servizio in relazione agli specifici contesti operativi;
- attuare operazioni sui file dei file system e sui file system stessi per soli scopi di manutenzione del sistema, indagine diagnostica, installazione di applicazioni o di tool diagnostici o gestionali, tuning, salvataggio, anche temporaneo, di dati e configurazioni, ripristino di condizioni normali di funzionamento.

3.2 Amministratori di rete (ADS – AR)

Gli Amministratori di Sistema con profilo di autorizzazione di amministratore di rete sono autorizzati ad operare su tutti i sistemi di rete compresi i sistemi di servizio (DHCP, DNS, VPN Server, WCS, ecc.) e sono tenuti a svolgere le seguenti attività:

- sorvegliare il corretto funzionamento dei sistemi in senso generale (monitoraggio) e dei sottosistemi specifici in particolare (CPU, memorie, sistemi dischi, storage, schede di rete, sistema di alimentazione e di ventilazione, ecc.);
- sorvegliare il corretto funzionamento dei servizi applicativi erogati attraverso i sistemi di rete tramite il monitoraggio dei log e dei messaggi prodotti dal sistema operativo e dal software di base;

- intervenire ogni qualvolta venga evidenziato un malfunzionamento, un guasto o una anomalia funzionale sui sistemi, sul software di servizio a bordo dei medesimi, sui servizi erogati tramite la infrastruttura di rete, per diagnosticare il problema e ripristinare il corretto funzionamento dei sistemi;
- intervenire periodicamente per verificare e, compatibilmente con i vincoli introdotti dall'hardware di sistema e dalle licenze disponibili, aggiornare il sistema operativo, i driver di periferiche, ed ogni componente del software di base per garantire l'allineamento della piattaforma con le versioni emesse dal produttore / costruttore;
- provvedere alla configurazione ottimale del sistema per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità/onerosità di gestione e mantenimento nel tempo delle funzioni;
- verificare quotidianamente il buon esito dei salvataggi dei dati giornalieri (backup) gestiti dallo specifico sistema e definire e garantire il salvataggio periodico delle configurazioni della piattaforma in particolare a seguito di modifiche;
- intervenire prontamente in situazioni di emergenza o in caso di manutenzione ordinaria o straordinaria per segnalare i bisogni dell'organizzazione ai fornitori esterni dell'assistenza tecnica, coordinare e seguire gli interventi relativi, informare gli utenti e le strutture tecniche coinvolte;
- segnalare eventuali problematiche dei sistemi o situazioni anomale ai dirigenti della UO Tecnologie Sanitarie, Informatiche Sanitarie e di Rete;
- definire e configurare gli utenti, gli account che devono operare sul sistema ed i parametri relativi, attribuendo loro il profilo di autorizzazione indicato dal Responsabile del trattamento cui il sistema è di supporto;
- cooperare all'installazione dei sistemi, monitorare la loro continuità operativa e la fruibilità continuativa dei servizi da parte degli utenti, verificare la funzionalità delle interfacce e attivare e disattivare i singoli processi software per garantire detta continuità di servizio in relazione agli specifici contesti operativi.

3.3 Amministratori di database (ADS – DBA)

Gli Amministratori di Sistema con profilo di autorizzazione di amministratore di database sono autorizzati ad operare su tutti (o parte – si veda ampiezza del profilo assegnato mediante lettera di designazione) i sistemi database Oracle e sono tenuti a svolgere le seguenti attività:

- sorvegliare il corretto funzionamento dei sistemi di database, delle varie istanze e delle utenze relative;
- sorvegliare il corretto funzionamento dei sistemi applicativi afferenti alla base di dati tramite il monitoraggio dei log e dei messaggi prodotti dal sistema database;
- intervenire ogni qualvolta venga evidenziato un malfunzionamento, un guasto o una anomalia funzionale sui sistemi database, sul software applicativo che vi afferisce, sui servizi che li usano, per diagnosticare il problema e ripristinare il corretto funzionamento del sistema RDBMS;
- intervenire periodicamente per verificare e, compatibilmente con i vincoli introdotti dai sistemi applicativi ospiti, aggiornare il sistema database ed ogni suo componente per garantire l'allineamento del sistema con le versioni emesse dal produttore / costruttore;
- provvedere alla configurazione ottimale del sistema per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità/onerosità di gestione e il mantenimento nel tempo delle funzioni;

- verificare il buon esito dei salvataggi dei dati giornalieri (backup) gestiti dallo specifico sistema e definire e garantire il salvataggio periodico delle configurazioni della piattaforma in particolare a seguito di modifiche;
- intervenire prontamente in situazioni di emergenza o in caso di manutenzione ordinaria o straordinaria per segnalare i bisogni dell'organizzazione ai fornitori esterni dell'assistenza tecnica, coordinare e seguire gli interventi relativi, informare gli utenti e le strutture tecniche coinvolte;
- segnalare eventuali problematiche dei sistemi o situazioni anomale ai dirigenti del UO TIR;
- definire e configurare gli utenti, gli account che devono operare sul sistema ed i parametri relativi, attribuendo loro un profilo coerente con il profilo di autorizzazione indicato dal Responsabile del trattamento per il trattamento relativo;
- cooperare all'installazione dei sistemi, monitorare la loro continuità operativa e la fruibilità continuativa dei servizi da parte degli utenti, verificare la funzionalità delle interfacce e attivare e disattivare i singoli processi software per garantire detta continuità di servizio in relazione agli specifici contesti operativi;
- attuare operazioni sulle strutture interne del database per soli scopi di manutenzione del sistema, indagine diagnostica, installazione di tablespace o di tool diagnostici o gestionali, tuning, salvataggio, anche temporaneo, di dati e configurazioni, ripristino di condizioni normali di funzionamento.

3.4 Sistemisti Gestori Applicativi (ADS – SGA)

Gli Amministratori di Sistema con profilo di autorizzazione di Gestore Applicativo sono autorizzati ad operare sui sistemi utilizzati dal trattamento di cui sono referenti applicativi e sono tenuti a svolgere le seguenti attività:

- sorvegliare il corretto funzionamento del sistema applicativo principale e di quelli ad esso interconnessi tramite il monitoraggio dei log e dei messaggi prodotti dal sistema applicativo e dal software di base su cui è montato;
- intervenire ogni qualvolta venga evidenziato un malfunzionamento, un guasto o una anomalia funzionale sui sistemi, sul software applicativo a bordo dei medesimi, sui servizi erogati tramite la piattaforma, per diagnosticare il problema e ripristinare il corretto funzionamento del trattamento. Qualora il referente applicativo non disponesse delle necessarie competenze sui sottosistemi tecnologici è tenuto a segnalare il problema agli amministratori di sistema, di database, di piattaforma o di rete competenti;
- intervenire periodicamente per verificare la compatibilità del trattamento/applicazione con gli aggiornamenti del sistema operativo, dei driver di periferiche, e di ogni componente del software di base per garantire l'allineamento della piattaforma con le versioni dei sistemi operativi e dei software di base emesse dai produttori / costruttori;
- provvedere alla configurazione ottimale del sistema, compatibilmente con le indicazioni del fornitore, per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità/onerosità di gestione e mantenimento nel tempo delle funzioni;
- intervenire prontamente in situazioni di emergenza o in caso di manutenzione ordinaria o straordinaria per segnalare i bisogni dell'organizzazione ai fornitori esterni dell'assistenza tecnica, coordinare e seguire gli interventi relativi, informare gli utenti e le strutture tecniche coinvolte;

- segnalare eventuali problematiche dei sistemi o situazioni anomale ai dirigenti della UO Tecnologie Sanitarie, Informatiche Sanitarie e di Rete;
- definire e configurare gli utenti (o richiederne la configurazione se il servizio è gestito in outsourcing), gli account che devono operare sul sistema ed i parametri relativi, attribuendo loro il profilo di autorizzazione indicato dal Responsabile del trattamento cui il sistema è di supporto;
- cooperare all'installazione dei sistemi, monitorare la loro continuità operativa e la fruibilità continuativa dei servizi da parte degli utenti, verificare la funzionalità delle interfacce e attivare e disattivare i singoli processi software per garantire detta continuità di servizio in relazione agli specifici contesti operativi;
- attuare operazioni sui dati per soli scopi di elaborazione dati (su richiesta dei responsabili dei trattamenti), manutenzione del sistema, indagine diagnostica, installazione di moduli applicativi o di tool diagnostici o gestionali, tuning, salvataggio, anche temporaneo, di dati e configurazioni, ripristino di condizioni normali di funzionamento.

4. Misure organizzative

Data la caratterizzazione tipica degli amministratori di sistema riportata al capitolo precedente, si definiscono di seguito le misure organizzative utili a definire:

- modalità di valutazione delle caratteristiche soggettive al fine della individuazione
- strumenti e tempi di designazione ADS interni
- strumenti e tempi di designazione ADS outsourcer
- regime di conoscibilità interna degli ADS che trattano i dati dei lavoratori
- processo di autorizzazione degli ADS (concessione credenziali)

La documentazione inerente agli amministratori di sistema sarà conservata agli atti della UO Tecnologie Sanitarie, Informatiche Sanitarie e di Rete e sarà composta da:

1. registro degli amministratori di sistema (come da schema allegato 1)
2. nomine ADS sottoscritte per accettazione
3. eventuali comunicazioni a fornitori nominati Responsabili esterni di trattamento
4. documentazione in caso di iniziative formative ad hoc per ADS

4.1 Valutazione delle caratteristiche soggettive

La valutazione delle caratteristiche soggettive deve corrispondere a quanto previsto dal provvedimento del Garante: *"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",* ma non può, d'altro canto, non tenere conto della applicazione in itinere del provvedimento e degli aggiornamenti normativi a seguito dell'entrate in vigore del GDPR.
Ad oggi, molte funzioni di ADS sono svolte all'interno della organizzazione dal personale tecnico addetto a tali mansioni (cd. ADS interni), e quindi si dà atto del fatto che i requisiti fondamentali per l'attribuzione del ruolo di ADS sono quelli derivanti dalla qualifica professionale ricoperta.

Preme sottolineare che, trattandosi nel caso specifico di dipendenti pubblici, a sostegno della affidabilità dei professionisti si richiama:

- la procedura di reclutamento effettuata mediante selezione pubblica per titoli ed esami;
- il "Codice di comportamento dei dipendenti delle pubbliche amministrazioni" al quale ciascuno, in quanto pubblico dipendente, deve attenersi
- il "Codice disciplinare" previsto dai contratti collettivi nazionali, e pubblicato agli albi aziendali e sulla Intranet

Laddove l'amministratore di sistema avesse comportamenti non adeguati al compito assegnato, si rimanda a quanto previsto dal codice disciplinare in materia di inadempienza rispetto ai compiti di istituto.
I criteri enunciati portano a identificare quali ADS nell'Azienda USL di Imola i profili professionali di:

- collaboratore tecnico professionale senior / sett. informatico
- collaboratore tecnico professionale /sett. informatico
- assistente informatico
- analisti informatici

assegnati gerarchicamente e funzionalmente alla UO Tecnologie Sanitarie e Informatiche sanitarie e di Rete.
Si aggiungono a questi professionisti alcuni professionisti appartenenti ad altri ruoli professionali ai quali siano assegnati compiti di "sistemista gestore di applicativo".

4.2 Strumenti e tempi di designazione ADS interni

Gli ADS interni sono, successivamente all'adozione del presente disciplinare, designati quali incaricati del trattamento (ex art. 2 quaterdecies del Codice) con funzione di amministratore di sistema. La lettera di incarico è firmata dal Titolare dei trattamenti, nel caso di specie il Direttore Generale. Spetta al Responsabile dell'UOC Tecnologie Sanitarie, Informatiche Sanitarie e di Rete, previo coordinamento con il Responsabile della UO alla quale appartiene l'amministratore di sistema interno all'Azienda, di proporre al Direttore Generale gli amministratori di sistema interni all'Azienda da nominare.
In itinere, ogni evento inerente un nuovo incarico, cessazione, variazione derivanti da cause diverse sarà oggetto di coerente comunicazione tra l'ente e l'interessato e darà origine a corrispondente variazione nel registro degli ADS.
La nomina degli ADS non ha scadenza se non connessa alla cessazione della funzione e/o dal servizio.
Il Registro degli ADS (v. Allegato 1) viene confermato / revisionato annualmente e trasmesso al Direttore Generale dalla UOC Tecnologie Sanitarie, Informatiche Sanitarie e di Rete. In tale occasione si individua il permanere delle condizioni di nomina e/o accertate eventuali motivazioni di variazione.
L'elenco nominativo degli ADS, ovvero Registro degli ADS, è conservato agli atti della UOC Tecnologie Sanitarie, Informatiche Sanitarie e di Rete.

4.3 Strumenti e tempi di designazione ADS outsourcer

Gli ADS outsourcer sono designati secondo le modalità descritte al § 2 della presente politica e alla quale si rimanda.

4.4 Regime di conoscibilità degli ADS che trattano i dati dei lavoratori

Gli ADS che trattano i dati dei lavoratori sono specificatamente individuati, come da Allegato 1 Registro Amministratori di sistema ADS, e conoscibili a istanza del lavoratore

4.5 Processo di autorizzazione degli ADS (concessione credenziali)

Il processo di autorizzazione degli ADS è analogo a quanto previsto per ogni altra concessione di credenziali in azienda, è descritto nella "IOP04 – Istruzione operativa e moduli per la gestione delle Credenziali Elettroniche".

5. Descrizione delle misure a carattere tecnologico e monitoraggio

L'azienda USL di Imola, in considerazione della complessità del sistema informatico ed informativo aziendale, e della numerosità degli ADS interni ed esterni, ha ritenuto necessario adottare un sistema di "Log Collection". Nell'ottica indicata in premessa, anche in questo caso, è intenzione dell'ente cogliere questa opportunità per migliorare la qualità della gestione del sistema informatico/informativo. Si è stabilito, quindi, di far evolvere progressivamente il sistema di Log Collection in un vero e proprio sistema di Security Information Event Management (SIEM).
Sono stati attivati i log sui server di autenticazione, sui server per il controllo accessi e sui principali server che gestiscono i database patrimonio aziendale.
L'accesso alla consultazione dei log avviene attraverso un applicativo web a cui sono abilitati operatori con il ruolo di "Sistemisti S.O."
L'attività di verifica periodica da farsi almeno annualmente consisterà in:
- verifica di coerenza: il riscontro di coerenza tra i log rilevati dal sistema di log collection e gli amministratori nominati;
- controllo accessi: verifica accessi effettuati se coerenti con quanto previsto dalla nomina e se coerenti con la presenza in servizio.

6. Appendice

Allegato 1 – Registro Amministratori di Sistema ADS (schema)

Nominativo	Struttura appartenenza	Profilo	Ambito	Addetto al trattamento dei dati dei lavoratori

Nominativo	Struttura appartenenza	Profilo	Ambito	Addetto al trattamento dei dati dei lavoratori