Policy Amministratori di Sistema

A cura della SSD Tecnologie Informatiche

Revisione: v.01 del 18.10.2024

SOMMARIO

1. PREMESSA

Il presente documento contiene le principali raccomandazioni per il ciclo di gestione degli Amministratori di Sistema, nominati e da nominare, all'interno dell'Azienda Regionale di Coordinamento per la Salute (in seguito "ARCS" o "Azienda").

La nomina e il successivo controllo degli Amministratori di Sistema (in seguito AdS) è realizzato in conformità al Provvedimento del 27 novembre 2008, n. 300 e s.m.i. dell'Autorità Garante per la Protezione dei Dati Personali, come novellato nel 2009.

La presente policy fa parte dei documenti di *accountability* predisposti da ARCS per rendere le caratteristiche del funzionamento dei sistemi di protezione dell'azienda e costituisce:

- parte integrante delle politiche di sicurezza di ARCS;
- elemento di base per la gestione delle attività che comportano il trattamento di dati personali ai sensi della normativa a essi applicabile;
- una descrizione dei processi e delle procedure interne di controllo dell'operato degli AdS;
- istruzione formalizzata per gli autorizzati al trattamento (ai sensi dell'art. 29 del GDPR e dell'art 2-quaterdecies del Codice Privacy).

La policy descrive il processo di individuazione, di nomina, di gestione e di controllo che ARCS adotta per gli AdS.

2. SCOPO E AMBITO DI APPLICAZIONE

La policy ha lo scopo di assicurare la corretta gestione delle attività necessarie per la nomina, la gestione e il controllo dei soggetti rientranti nella categoria degli AdS conformemente alla normativa europea e nazionale in materia di protezione dei dati personali e ai provvedimenti emessi dall'Autorità Garante sul tema. Questa Policy si applica all'ARCS e nella fattispecie al personale coinvolto.

3. MODALITÀ OPERATIVE

3.1 GENERALITÀ

Il provvedimento del Garante della Privacy *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministrazione di sistema – 27 novembre 2008* [1] ha introdotto la figura tecnica dell'AdS.

[1] Con la definizione di amministratore di sistema si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente 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. Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

[Rif. MMS ABSC_ID 5.1.1] Sebbene ogni attività tecnica che comporti un'effettiva capacità di azione sulle informazioni va considerata a tutti gli effetti alla stregua di un trattamento di dati personali, non tutto il personale che opera sui sistemi può essere qualificato come AdS. La normativa, infatti, oltre a differenziare l'Amministratore dal semplice addetto alla manutenzione o da colui che si occupa dell'immissione dati, delinea un profilo che, per la particolare capacità di azione e la natura fiduciaria delle mansioni ad esso assegnate, deve possedere particolari requisiti tecnici e personali. Trattandosi di una figura professionale che si occupa della gestione e della manutenzione di un sistema di elaborazione e delle sue componenti, è possibile individuare, all'interno di una stessa organizzazione, tipologie specifiche di AdS, interne o esterne, differenziate per livello di autorizzazione e di profilo (vedi sezione Classificazione degli AdS).

Con il termine AdS si intendono quelle particolari figure professionali che per competenza, professionalità e riservatezza sono deputate alla gestione e alla manutenzione di un impianto di elaborazione dati, ivi compresi gli ambienti database, gli ambienti di rete e i gestori di applicativi complessi.

[Rif. MMS ABSC_ID 5.1.3] L'AdS è individuato per ciascun sistema in maniera puntuale, anche attribuendone la responsabilità in relazione alla correlata "tipologia" (ad esempio, sistemi Linux), evitando così una elencazione puntuale che diverrebbe rapidamente obsoleta.

Rif. MMS ABSC_ID 5.10.3] Gli AdS utilizzano le proprie credenziali nominative con diritti amministrativi di alto livello, per le sole operazioni che ne richiedano i privilegi; qualora il sistema non permetta l'utilizzo di credenziali nominative è consentito l'utilizzo di credenziali generiche (ad esempio *admin/administrator/root*) purché esista un registro del soggetto che ha operato con quella credenziale.

Durante lo svolgimento delle attività gli AdS sovraintendono, presiedono e monitorano, sotto la propria responsabilità e sulla base delle autorizzazioni loro delegate, specifiche fasi di lavoro o di processo che possono incidere sui diritti e sulle libertà dei soggetti che utilizzano i sistemi informatici.

Nel seguito, sono elencati un insieme di criteri per individuare l'applicabilità della qualifica di AdS (è condizione sufficiente ricadere in una delle fattispecie descritte):

- qualora sussista che un autorizzato possa accedere in modo indiscriminato ad un insieme di dati personali oltre quanto consentito agli utenti non privilegiati del sistema;
- qualora vi sia la possibilità di impostare privilegi/autorizzazioni di altri autorizzati;
- qualora vi sia la possibilità di installare software;
- qualora vi sia la possibilità di mutare la configurazione di un sistema.

semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente responsabili di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti in chiaro le informazioni medesime.

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

Gli AdS hanno di norma a disposizione funzioni che permettono la gestione e il monitoraggio degli altri utenti del sistema.

È prevista la registrazione degli accessi logici (c.d. autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli AdS; la stessa include i riferimenti temporali e la descrizione dell'evento che le ha generate. Tali registrazioni -*access log* e *system log*- devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

In virtù della convenzione in essere con la società in house della Regione, la registrazione e l'esportazione inerente la conservazione dei dati di log è gestita dal Responsabile del Trattamento ex art. 28 GDPR (Insiel), in modalità conforme alla vigente normativa.

[Rif. MMS ABSC_ID 5.1.4, ABSC_ID 5.5.1] Ogni sistema dispone di sistemi di tracciamento di tutti gli eventi generati automaticamente o dagli utenti. Gli Amministratori sono sottoposti a specifico log di accesso che permette di tenere sotto controllo:

- User ID: identificativo dell'utenza che sta effettuando l'accesso (es. utente, servizio, processo);
- Descrizione evento di autenticazione: sono da tracciare le azioni di log-in e log-out ivi compresi i tentativi di accesso;
- Sistema acceduto: descrizione/identificazione del target su cui è stato effettuato il log-in o il log-out;
- Sistema sorgente: i dati identificativi della linea di comunicazione e del terminale utilizzato (ove possibile);
- Timestamp: Data e ora dell'operazione (es. YYYY-MM-DD hh:mm:ss) indicante l'istante nel quale si è riscontrato l'evento tracciato;
- TimeZone: Il Timezone del server che ha generato il log (es. +hh:mm oppure –hh:mm). Il timezone è opzionale se il sistema è configurato con UTC +01:00, altrimenti deve essere espressamente indicato.

I *sistemi applicativi complessi* sono dei software che realizzano funzionalità utili ai processi aziendali; tali applicativi sono spesso caratterizzati dalla presenza di ruoli operativi che forniscono privilegi avanzati ad alcuni utenti, che devono pertanto essere nominati AdS.

Ogni sistema applicativo complesso può essere configurato con sistemi di tracciamento di tutti gli utenti. Anche per questi sistemi deve esistere uno specifico log di utilizzo. Rientrano in questa macro-classe:

- comandi amministrativi in genere;
- la natura e il dettaglio delle operazioni effettuate sulle applicazioni e sulle basi dati, anche se in sola consultazione (ove possibile);
- modifiche dei ruoli utente;
- attribuzioni di nuovi utenti;
- attribuzioni di ruoli utente ai singoli utenti;
- operazioni di reset o modifiche delle modalità di accesso degli utenti;
- gestione di eventuali sviluppatori esterni;

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

- gestione delle credenziali riservate di accesso (ci si riferisce a quelle inserite all'interno dell'applicativo software);
- Timestamp: Data e ora dell'operazione (es. YYYY-MMDD hh:mm:ss) indicante l'istante nel quale il server ha riscontrato l'evento tracciato;
- TimeZone: Il Timezone del server che ha generato il log (es. +hh:mm oppure –hh:mm). Il timezone è opzionale se il sistema è configurato con UTC +01:00, altrimenti deve essere espressamente indicato

Tali funzionalità non sono presenti in tutti gli applicativi complessi. Occorrerà, ove possibile in fase di manutenzione evolutiva, attuare modifiche applicative per sviluppare tali funzionalità. Per i futuri applicativi occorrerà prevedere un sottosistema di funzioni amministrative che permettano tali attività di controllo.

3.2 Classificazione degli AdS

I compiti di un AdS sono ampi. Ferma restando la possibilità di attribuire più profili alla stessa persona fisica, allo scopo di individuare puntualmente l'ambito di operatività del soggetto da nominare, vengono declinate le seguenti tipologie di AdS:

- **AdSb**: i soggetti deputati alla gestione degli accessi da parte del personale e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, nonché, in via residuale, tutti coloro che possiedono la qualifica di AdS e che non siano strettamente qualificabili quali DBA o NA;
- **DBA**: i soggetti deputati alla predisposizione dei data base su indicazioni dei gruppi di progetto e al monitoraggio degli stessi data base al fine di garantire il continuo esercizio. Il DBA è deputato, altresì, in collaborazione con le funzioni aziendali che gestiscono gli applicativi, a gestire lo spazio, ad effettuare i backup e i restore del database;
- **NA**: i soggetti preposti alla gestione delle risorse/attrezzature di rete e dei relativi protocolli;
- **ASA**: i soggetti deputati alla gestione di specifici software applicativi e/o complessi che sovraintendono, gestiscono, sviluppano, verificano e controllano le funzionalità di sicurezza inserite in detti applicativi e/o software complessi;
- **PdL**: i soggetti che gestiscono le postazioni di lavoro;
- **Post**: i soggetti che hanno la facoltà di installare software sulla propria postazione di lavoro;
- **VdS**: i soggetti deputati alla gestione dei sistemi di videosorveglianza;
- **VdC**: i soggetti deputati alla gestione dei sistemi di collaboration, videoconferenza e similari;
- **Fon**: i soggetti deputati alla gestione di sistemi di fonia;
- **Log**: i soggetti deputati alla gestione del SIEM e degli altri sistemi di logging;

3.3 Individuazione e nomina degli AdS

In ottemperanza a quanto prescritto dall'Autorità Garante, ARCS, nella persona del Direttore Generale, procede alla nomina degli AdS sulla base delle proposte avanzate dai Direttori di Struttura i quali, previa valutazione dei requisiti di affidabilità, capacità, competenza ed esperienza da effettuarsi con il supporto della struttura Tecnologie informatiche, individuano i soggetti da nominare nonché l'ambito di operatività e di trattamento necessari alle funzioni svolgere.

INDIVIDUAZIONE

L'AdS è individuato dai Direttori di Struttura Semplice, Dipartimentale e Complessa che dettagliano, con il supporto della struttura Tecnologie informatiche, il ruolo e gli ambiti di operatività consentiti in base al profilo di autorizzazione e previa valutazione del rischio[2] insito nelle mansioni da assegnare.

[Rif. MMS ABSC_ID 5.1.1] I soggetti vanno individuati tenendo conto del seguente requisito previsto dall'Autorità Garante della privacy "*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.*"

Ai fini della valutazione dei requisiti di capacità ci si può basare sull'esperienza maturata, possibilmente suffragata da evidenze oggettive rinvenibili in certificazioni che possono essere relative alla specifica tecnologia oggetto delle attività (per esempio certificazioni Microsoft sui diversi prodotti) o alla tematica della sicurezza (per esempio Auditor ISO 27001).

Come requisiti minimali, derogabili in singoli casi motivati, si individuano:

- Diploma tecnico specifico, con almeno due anni di esperienza;
- Laurea tecnica specifica, con almeno sei mesi di esperienza.

NOMINA

[Rif. MMS ABSC_ID 5.10.2] La nomina dell'AdS sarà in ogni caso individuale e conterrà in modo specifico il ruolo e gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

L'AdS è nominato, secondo il modello allegato alla presente policy, dal Direttore Generale sulla base delle proposte avanzate dai rispettivi Direttori di Struttura sulla base di quanto sopra descritto.

Le funzioni attribuite all'AdS sono contenute nell'atto di nomina che dovrà essere sottoscritto dall'AdS stesso insieme all'informativa e all'autorizzazione specifica al trattamento dei dati, da consegnarsi al Direttore della propria struttura di afferenza.

[Rif. MMS ABSC_ID 5.2.1] Ogni Direttore di Struttura è tenuto a mantenere aggiornato il proprio elenco degli AdS e a trasmettere copia dell'atto di nomina, tutte le successive variazioni, alla Struttura Risorse Umane -che lo conserverà nel fascicolo del dipendente- e alla Struttura Tecnologie Informatiche -che provvederà ad aggiornare l'elenco degli AdS con le nuove nomine- pubblicandolo in Bacheca.

[2] Dal Provvedimento AdS: Ai fini del presente 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. Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

3.4 Formazione ed aggiornamento

Al fine di migliorare il livello di sicurezza dell'organizzazione, l'Azienda organizza periodicamente sessioni di formazione ed aggiornamento sui temi della sicurezza nel trattamento dei dati, nei quali vengono trattate tematiche specifiche connesse ai compiti di AdS.

3.5 Revoca della nomina

L'Azienda può revocare l'incarico di AdS in caso di:

- inadempienza o inosservanza delle prescrizioni di sicurezza;
- violazione della presente Policy;
- sopravvenuta mancanza dei requisiti necessari per ricoprirne il ruolo;
- modifica del rapporto contrattuale di lavoro dell'AdS.

In considerazione ai risvolti tecnici, ma soprattutto alla continuità ed affidabilità dei servizi, la revoca dell'incarico di un AdS dovrà seguire la seguente procedura:

- verificare l'esistenza di eventuali servizi avviati (erroneamente) con l'account dell'AdS ed eventualmente assegnare al servizio un account specifico per l'esecuzione della tipologia di servizi interessata;
- controllare l'esistenza di eventuali backdoor (account o applicative, accessi remoti, autorizzate o non autorizzate) riferibili all'AdS da disabilitare;
- nel caso non sia già esistente, creare un account amministrativo con lo stesso profilo di autorizzazione dell'AdS da disabilitare, da assegnare al nuovo AdS (sostituto);
- disabilitare l'account dell'AdS revocato;
- verificare che tutti i servizi collegati al profilo di autorizzazione dell'AdS risultino perfettamente funzionanti;
- segnalare alla persona fisica, se in servizio, la disabilitazione dell'account di AdS e la revoca dell'incarico.

3.6 Affidamento del ruolo di AdS a soggetti esterni

Qualora l'Azienda decida di affidare, in toto o in parte, la gestione di alcuni servizi che implichino il ruolo di AdS, dovrà sottoscrivere una nomina ex art. 28GDPR, qualificando il fornitore come Responsabile del trattamento dei dati.

Il Responsabile del trattamento è tenuto all'individuazione e alla nomina dei propri AdS ed è altresì onere dello stesso provvedere all'eventuale revoca delle nomine effettuate.

Nel caso di affidamento di servizi che implicano la gestione di sistemi, il Responsabile di Commessa (RUP/DEC) dovrà:

- specificare che il servizio prevede il ruolo di AdS;
- istruire il fornitore a configurare i sistemi secondo le misure di sicurezza applicabili e per alimentare i log;
- chiedere l'elenco dei sub responsabili;
- chiedere l'elenco degli AdS solamente in fase di audit.

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

3.7 Elenco degli AdS

[Rif. MMS ABSC_ID 5.2.1] Per una più immediata ed efficace gestione degli AdS, ARCS, per il tramite della Struttura Tecnologie Informatiche, predispone un elenco contenente le nomine effettuate.

L'utilità di un elenco degli AdS è comprovata dalla presenza dell'obbligo di mantenere aggiornato e rendere disponibile -in caso di accertamenti dell'Autorità Garante- l'identità dei soggetti preposti ad amministrare i sistemi.

L'Azienda è, inoltre, tenuta ad informare i lavoratori circa l'identità degli AdS qualora questi effettuino attività che comprendono il trattamento dei dati personali di dipendenti, collaboratori e soggetti terzi; a tal fine, l'elenco viene pertanto pubblicato in un'area dello storage accessibile a tutti i dipendenti (bacheca lettura).

3.8 Monitoraggio delle attività degli AdS

ARCS, per il tramite dei servizi erogati da Insiel S.p.A., usufruisce di strumenti automatizzati per il tracciamento dell'operato informatico a tutela dell'integrità, disponibilità e riservatezza dei sistemi informatici stessi.

Sarà cura del DPO aziendale verificare che siano state messe in atto le registrazioni previste. Tutti i controlli devono essere in linea con le prescrizioni previste dall'Autorità Garante e possono essere effettuati solo sugli AdS che hanno ricevuto esplicita autorizzazione, ai sensi dell'art. 29 del RGPD.

3.9 Controlli

Il DPO provvede a verificare i log degli AdS per verificare, a campione, eventuali anomalie e/o per verificare che gli stessi Amministratori abbiano rispettato gli ambiti di operatività consentiti. L'azienda si riserva la possibilità di effettuare controlli a campione sugli Amministratori nominati dando un preavviso minimo di 7 giorni dalla data di verifica.

Dalla verifica potranno emergere richieste che dovranno essere portate all'attenzione del Titolare per le azioni successive. Vista la particolare criticità del ruolo, in caso di anomalie che siano definibili gravi per il non rispetto delle indicazioni impartite, in fase di verifica si potrà disporre la sospensione temporanea delle credenziali e delle funzioni di AdS comunicando, con relazione dettagliata, i motivi e le evidenze delle anomalie riscontrate. Sarà eventualmente compito del Titolare decidere se procedere con atti sanzionatori formali verso l'AdS.

Ogni AdS deve produrre annualmente al Direttore della propria struttura di afferenza una relazione sulle proprie attività, segnalando quelle che potrebbero avere avuto impatti rilevanti sugli interessati (ossia tutti gli utenti dei sistemi e applicazioni amministrate).

Tale relazione dovrà includere:

- le misure di sicurezza non adottate, o adottate con deroghe anche parziali;
- suggerimenti per l'adozione di ulteriori misure di sicurezza oppure la diversa realizzazione delle misure esistenti;
- giustificazione di eventuali accessi effettuati al di fuori dell'orario di lavoro;
- attestazione di regolari controlli sulle utenze, per verificare la corretta gestione del ciclo di vita delle stesse.

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

4. RACCOMANDAZIONI GENERALI PER GLI AMMINISTRATORI DI SISTEMA

Le seguenti raccomandazioni generali valgono per tutti gli AdS a prescindere dal tipo di sistema che è posto sotto la loro autorità:

- *[Rif. MMS ABSC_ID 5.1.2, ABSC_ID 5.1.3, ABSC_ID 5.10.1]* assegnare a ciascun AdS credenziali distinte in modo da assicurare la completa separazione tra utenze privilegiate e non privilegiate:
  - una utenza standard: questa utenza dovrà essere usata durante il normale operato del dipendente "amministratore di sistema", ossia nei casi in cui non siano richiesti privilegi particolari per svolgere le proprie mansioni;
  - una (o e se tecnicamente richiesto più) utenza amministrativa quale AdS: tale utenza dovrà essere strettamente usata nei casi in cui si richiedono privilegi ulteriori per poter svolgere il proprio operato, ovvero quando si necessiteranno diritti di amministrazione sul sistema su cui si sta operando;
- *[Rif. MMS ABSC_ID 5.1.3]* assicurare che i profili di accesso, in particolare per le utenze con privilegi amministrativi, rispettino il principio del need-to-know, ovvero che non siano attribuiti diritti superiori a quelli realmente necessari per eseguire le attività di lavoro. Le utenze con privilegi amministrativi devono essere utilizzate per il solo svolgimento delle funzioni assegnate;
- *[Rif. MMS ABSC_ID 5.3.1]* prima di introdurre in rete dei nuovi dispositivi, sostituirne le credenziali di amministrazione predefinite e, se possibile, collegarle al sistema di gestione centralizzato delle credenziali, ovvero sostituirle con le credenziali in linea con le password policy attuali;
- *[Rif. MMS ABSC_ID 5.6.1, ABSC_ID 5.7.1-3-4-5]* obbligo di associare alle utenze amministrative, password di adeguata complessità nel rispetto delle "best practices" vigenti attivando, ove possibile, l'autenticazione multi-fattore. In ogni caso le password non possono avere una durata superiore ai 30 giorni. È reputato accettabile, a titolo di eccezione, estendere questo tempo a 90 giorni per gli amministratori di sistemi applicativi complessi che non dispongono di sistemi di gestione dei log;
- *[Rif. MMS ABSC_ID 5.7.6]* divieto di assegnare utenze amministrative generiche e/o già attribuite, anche in tempi diversi;
- *[Rif. MMS ABSC_ID 5.11.1]* assegnare in ciascun sistema ad almeno 2 soggetti distinti il ruolo di AdS, in modo da poter garantire la necessaria continuità operativa in caso di assenze ed impedimenti. Ove tale assegnazione non risulti tecnicamente possibile, l'AdS deve comunicare al Direttore della Struttura di afferenza, in busta chiusa sigillata con data di consegna e firma autografa, le credenziali di una utenza di livello amministrativo in grado di operare, in caso di indisponibilità dell'Amministratore stesso, sul sistema in oggetto. L'utenza di emergenza deve poter essere utilizzata per il tempo di validità della busta (tecnicamente, occorre interrompere la decadenza della password). Tali buste dovranno essere conservate in una cassaforte in plico riservato che può essere aperto solo in presenza contemporanea di due Direttori di Struttura o del Direttore della Struttura di afferenza e del DPO. Qualora si rendesse necessario aprire la busta, sarà onere del Direttore della Struttura di afferenza dell'AdS verbalizzare l'evento riportandone la motivazione.
- evitare l'uso di credenziali "built in", quali root/administrator, se non in caso di accertata impossibilità ad operare in altro modo. Tali credenziali dovranno essere custodite in modalità sicura (cifrate e/o custodite in luogo chiuso a chiave);

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

- le credenziali amministrative non devono essere conservate in chiaro sui sistemi, ma devono essere adottati sistemi di cifratura (ad es. conservazione dell'hash MD5) per garantirne la riservatezza e la disponibilità;

5. INDICAZIONI FINALI

Questa policy, così come gli atti periodici che ne derivano, contribuiscono a definire l'accountability del Titolare del trattamento dei dati.

Tutta la documentazione deve essere conservata per almeno 5 anni dalla data di cessazione del mandato dell'AdS.

La presente procedura e le relative istruzioni potranno essere soggette ad aggiornamenti ed integrate con ulteriori e dettagliati documenti di carattere operativo e tecnico, in funzione anche di mutamenti normativi o innovazioni introdotte a livello aziendale.

6. RIFERIMENTI NORMATIVI

Allo scopo di rappresentare il quadro normativo di riferimento si elencano le principali fonti normative in materia.

Normativa europea

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Normativa nazionale

- D. Lgs. n.30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", così come modificato dal D. Lgs. n. 101 del 2018 e ss.mm.ii.
- D. Lgs. n.138 del 4 settembre 2024 recante "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE)"

Provvedimenti del Garante per la Protezione dei Dati Personali e dell'European Data Protection Board

- Garante per la protezione dei dati personali, Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema del 27 novembre 2008 e ss.mm.ii (il documento è disponibile in forma integrale e con le FAQ dedicata presso la pagina web https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499)
- Linee Guida Privacy by design dell'EDPB

Decreti e Delibere Agenzia per la Cyber Security Nazionale (ACN)

- Determina n. 306 del 18 gennaio 2022
- Decreto direttoriale Prot. n. 29 del 1 febbraio 2023

- Decreto direttoriale Prot. n. 54 del 8 febbraio 2023
- Determinazione n. 307 del 18 gennaio 2022

Standard applicabili

- Misure minime di Sicurezza per le pubbliche amministrazioni ICT Agid secondo la direttiva del Presidente del Consiglio dei ministri (agosto 2015)
- Framework Nazionale per la Cyber Security e la Data Protection Edizione 2019
- Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi Cloud per la Pubblica Amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi Cloud per la Pubblica Amministrazione
- Determinazione 220 del 17 maggio 2020 Linee Guida – "La Sicurezza nel Procurement ICT"
- Cloud Security Alliance STAR Level 2

7. DISPOSIZIONI FINALI, ENTRATA IN VIGORE E PUBBLICITÀ

La policy entra in vigore dalla data di esecutività del relativo ecreto di adozione.

Con l'entrata in vigore della presente Policy, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti. Per quanto non espressamente previsto sarà fatto riferimento alla normativa vigente in materia.

La policy sarà portata a conoscenza di tutti gli utenti dell'Azienda attraverso la pubblicazione sul sito Internet aziendale nella sezione "Atti amministrativi generali" e su una unità di rete accessibile a tutti gli utilizzatori. Verrà, inoltre, trasmessa specifica nota informativa a tutte le strutture aziendali.

8. NOTIFICHE DI NON CONFORMITÀ, MISURE DISCIPLINARI E SANZIONI

Dipendenti e collaboratori dell'ARCS sono tenuti a rispettare pienamente la presente Policy.

È fatto obbligo di adeguare i propri comportamenti alle disposizioni previste. Il mancato rispetto o la violazione delle regole sopra richiamate è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari e risarcitori previsti dalla normativa applicabile.

9. AGGIORNAMENTO DELLA POLICY

La presente policy è approvata dal Direttore Generale ed è sottoposta a revisione ed aggiornamento come conseguenza delle modifiche necessarie all'adeguamento e/o miglioramento del processo stesso; ad intervalli periodici, è prevista la revisione del documento per verificarne l'adeguatezza. Il mantenimento, l'aggiornamento e qualsiasi modifica alla Policy di AdS deve essere esaminata ed approvata coerentemente con quanto indicato dal Reg. UE 2016/679 e con i processi organizzativi dell'ARCS.

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

La policy verrà, altresì, aggiornata ogni qualvolta si verifichi almeno una delle seguenti condizioni:

- identificazione di nuovi rischi o minacce/modifiche rispetto a quanto considerato in una precedente attività di analisi del rischio;
- incidenti di sicurezza correlati alla gestione della sicurezza informatica;
- evoluzione del contesto normativo e legislativo in materia di sicurezza.

10. Ruoli e Responsabilità

Si rappresenta nel seguito la matrice RACI della presente policy.

Fasi/Attività \ Soggetti	Titolare del Trattamento	Direttori di Struttura SS, SSD, SC	Struttura Gestione Risorse Umane	SSD T.I.	Ufficio Privacy	DPO
Individuazione AdS		A/R		C		
Nomina AdS	A	R	I	C	C	
Tenuta elenco AdS				A/R		I
Monitoraggio attività AdS				C	C	A/R
Audit a campione					C	A/R

Legenda:

R (***Responsible***) è colui che segue e assegna l'attività;
A (***Accountable***) è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato
C (***Consulted***) è la persona che aiuta e collabora con il *Responsible* per l'esecuzione dell'attività;
I (***Informed***) è colui che deve essere informato, al momento dell'esecuzione dell'attività o (spesso) al suo completamento

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

11. Termini, Acronimi e Definizioni

Termine/Acronimo	Definizione
Accesso informatico	capacità da parte di un soggetto (utente o processo) di effettuare operazioni (lettura, aggiornamento, scrittura, comunicazione) su "oggetti" informatici (applicazioni, programmi, dati);
Account	insieme di funzionalità, strumenti e contenuti attribuiti ad un nome Utente in determinati contesti operativi, non solo in siti web o per usufruire di determinati servizi su Internet ma anche per accedere alle applicazioni software
Amministratore di Sistema ("AdS")	Figura professionale dedicata alla gestione e alla manutenzione di attrezzature di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
Amministratore di software Applicativo Complesso (ASA)	È il soggetto deputato alla gestione di specifici software applicativi complessi che sovraintende, gestisce, sviluppa, verifica e controlla la sicurezza di detti applicativi software complessi anche attraverso la gestione di appositi contratti di assistenza.
Autorità Garante	L'Autorità Garante per la protezione dei dati personali. Autorità di cui all'art.153 del Codice Privacy, "Il Garante" istituita dalla Legge n.675 del 31/12/1996;
Autorizzati	Persone fisiche autorizzate al trattamento dei dati personali e che operano in base alle istruzioni fornite dal titolare.
Backup	indica la replicazione su un qualunque supporto di memorizzazione di materiale informativo archiviato nella memoria di massa dei Computer, siano essi Personal Computer, workstation, server, tablet, smartphone, ecc. al fine di prevenire la perdita definitiva dei dati in caso di eventi malevoli accidentali o intenzionali
Codice Privacy	Codice in materia di protezione dei dati personali di cui al D. Lgs. 196/2003 nella versione vigente.
Credenziali di autenticazione	le informazioni e/o i dispositivi, in possesso di una persona, solo da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica
Data Breach	Deve intendersi la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Database Administrator ("DBA")	È il soggetto preposto alla gestione degli accessi, alla predisposizione delle tabelle, degli indici e delle viste di un determinato ambiente database.
Database Management System	Un Database Management System, abbreviato in DBMS o Sistema di gestione di basi di dati, è un sistema software progettato per consentire la creazione, la manipolazione e l'interrogazione efficiente di database, per questo detto anche "gestore o motore del database"
Dati particolari	I dati personali idonei a rilevare l'origine razziale ed etnica, le opinioni politiche, le convenzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale dell'interessato.
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, attraverso un identificativo come il nome, un

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

Termine/Acronimo	Definizione
	numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Dati relativi a condanne penali e a reati	I dati personali relativi a condanne penali ai reati o alle connesse misure di sicurezza.
DEC	Direttore Esecutivo Contratto: come definito dal D. Lgs.36/2023, art. 114: delegato dal RUP alla verifica della corretta esecuzione dell'appalto
Destinatario	La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
DPO (RPD)	Data Protection Officer, figura introdotta dal Regolamento generale sulla protezione dei dati 2016/679, svolge attività di consulenza e controllo sui trattamenti.
GDPR (RGPD)	Regolamento Generale sulla Protezione dei Dati – Regolamento (UE) 2016/679
Interessato	Persona fisica, identificata o identificabile, a cui si riferiscono i dati personali. In particolare, i soggetti interessati al trattamento dei dati personali da parte sono, a titolo esemplificativo e non esaustivo, i dipendenti, collaboratori, i consulenti e liberi professionisti, i clienti e i fornitori, anche potenziali.
Firewall	dispositivo hardware/software per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi
Freeware	categoria di software proprietario il cui utilizzo è concesso a titolo gratuito
INSIEL	Informatica per il Sistema di Enti Locali S.p.A., è una società in-house della Regione Friuli-Venezia Giulia che si occupa della realizzazione degli sviluppi e della conduzione del SISSR
LAN	Local Area Network, è un gruppo di computer connessi in un'area locale per comunicare tra loro e condividere risorse quali le stampanti, ecc…
Log	Registro cronologico degli eventi. Sistema/report di tracciamento delle attività svolte su un sistema o un'applicazione che contiene il time stamp dell'evento e la descrizione strutturata dell'evento, oltre le informazioni sull'utente che lo ha generato.
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.
Network Administrator (NA)	È il soggetto preposto alla gestione dei sistemi di elaborazioni effettuati tramite le risorse di rete, nonché sovraintende, gestisce, sviluppa, verifica e controlla la sicurezza delle reti e dei relativi protocolli.
Dirigente/Responsabile/Direttore della Struttura di afferenza	Soggetto di vertice nell'ambito delle quali sono effettuate operazioni di trattamento rilevanti e al quale vengono attribuiti, in virtù della sua funzione, esperienza e competenza, i compiti necessari per garantire che le già menzionate operazioni di trattamento siano conformi alle direttive, prassi e policy aziendali, nonché alla normativa vigente in materia di protezione dei dati personali.

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

Termine/Acronimo	Definizione
Responsabile di Commessa	Soggetto che è responsabile dell'erogazione dei servizi nell'ambito di un ordine cliente
Responsabile di Offerta	Soggetto che predispone la proposta tecnico economica verso un cliente
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento. La nomina dovrà essere disciplinata da un contratto o da un altro atto giuridico che vincoli quest'ultimo al Titolare e che disciplina la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di dati trattati e le categorie di interessati, nonché gli obblighi e i diritti del Titolare del trattamento (art. 28, RGPD).
Risorse Umane	Svolge attività di analisi, misurazione e valorizzazione delle capacità e competenze del personale e garantisce l'aggiornamento delle informazioni inerenti al personale. Cura l'elaborazione e l'aggiornamento dei regolamenti interni e delle procedure gestionali in materia di conferimento di incarichi nonché delle procedure/istruzioni in materia di gestione ed organizzazione del personale interfacciandosi anche con le altre strutture aziendali per ambiti di competenza.
RUP	Responsabile Unico del Procedimento come definito dalla Legge 241/90, art. 31. Il concetto è ripreso dai Codice degli Appalti D. Lgs. 36/2023, che lo identifica come Responsabile Unico del Progetto (art. 15).
Outsourcing	Esternalizzazione, consiste nell'affidare un incarico a una società esterna specializzata in una fase o attività tipica della propria azienda
Profilo di autorizzazione	insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti
Recovery	Recupero di materiale informatico precedentemente transitato e/o cancellato su dispositivi informatici, come un computer. Può essere necessario a seguito di un danno logico o di un danno fisico.
Sistema di Autenticazione	le informazioni e/o i dispositivi, in possesso di una persona, solo da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica
Sistema Operativo	Software di sistema che gestisce le risorse hardware e software della macchina e fornisce servizi in base ai software applicativi (cioè i programmi) installati
Sistema informatico	Individua una macchina fisica o un insieme di macchine fisiche che definiscono una o più macchine logiche (virtuali) che realizzano lo stesso gruppo di funzionalità. Ogni sistema ha sempre un sistema operativo e un software di base. Ogni sistema/ecosistema è basato su un sistema operativo di virtualizzazione dove sono configurate una o più macchine con proprio sistema operativo e proprio software di base. Ogni sistema dispone di un amministratore che dispone di tutte le autorizzazioni di configurazione e monitoraggio degli utenti sopra definiti. Il concetto nel gergo comune può individuare una funzionalità automatizzata che comprende anche una componente applicativa
Sistema Privacy	L'insieme delle procedure, della modulistica, delle istruzioni operative, delle misure e di quant'altro predisposto, per garantire la sicurezza delle informazioni e la gestione dei trattamenti dei dati, in conformità al RGPD e alle ulteriori disposizioni e provvedimenti applicabili in materia di protezione dei dati personali.

ARCS Azienda Regionale di Coordinamento per la Salute
Sede legale: Udine – Via Pozzuolo 330 Tel.: + 39 0432/1438010
P. IVA/C.F. 02948180308 PEC: arcs@certsanita.fvg.it

Termine/Acronimo	Definizione
Scripting	Il termine script designa un tipo particolare di programma scritto con un linguaggio di scripting; la distinzione tra script e programmi normali non è netta e univoca, generalmente però uno script è caratterizzato da complessità relativamente bassa, utilizzo di un linguaggio interpretato, utilizzo per un processo di configurazione automatizzata del sistema, linearità, richiamo di altri script o programmi, mancanza di un'interfaccia grafica
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Trattamento di dati personali	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Wiki	Raccolta di documenti, generalmente collegati fra loro (ipertestuali) o comunque racchiusi in un determinato database o repository (ambiente in cui sono gestiti dati), relativamente a una determinata tematica

12. ALLEGATI

- Modello atto di nomina
- Informativa ex art. 13 GDPR
- Autorizzazione per il trattamento di dati in qualità di AdS