ALLEG. 3

Azienda Sanitaria Locale Salerno

Procedura per la Gestione delle Utenze del personale interno ed esterno

Storia del documento

Data	Versione	Descrizione modifiche	Autore
04.03.2019	1.0	Prima stesura	
14.03.2019	2.0	Revisione	

27

Indice

1 Introduzione 3

1.1 Scopo del documento 3

1.2 campo di applicazione 3

1.3 Riferimenti 4

1.4 Definizioni 4

2 Overview del Processo 5

2.1 Tipologie di utenze 5

2.2 Ruoli e responsabilità 6

3 Descrizione del Processo 7

3.1 Creazione dell'Utenza 9

3.2 Reset dell'Utenza 11

3.3 Modifica dei privilegi Sull'Utenza 12

3.4 Disabilitazione dell'Utenza 15

3.5 Revisione periodica delle utenze attive 16

Indice delle Tabelle

Tabella 1 – Definizioni 4

Tabella 2 – Ruoli e Responsabilità 6

Tabella 3 – Legenda 8

Tabella 4 – Flow-chart e Matrice – Attivazione Utenza 10

Tabella 5 – Flow-chart e Matrice – Reset Utenza 12

Tabella 6 – Flow-chart e Matrice –Modifica dei privilegi Utenza 14

Tabella 7 – Flow-chart e Matrice – Disabilitazione Utenza 15

Tabella 8 – Flow-chart e Matrice – Controllo periodico Utenze 17

28

1 INTRODUZIONE

Il Regolamento UE 2016/679 (di seguito GDPR o Regolamento) nasce con lo scopo di tutelare i dati personali delle persone fisiche. il regolamento sostituisce integralmente quanto sancito nel decreto legislativo 196/2003 – detto anche codice privacy – che viene integralmente conformato al GDPR attraverso il d. lgs. 101/2018. punto principale da cui partire è la mancanza di indicazioni mandatorie per i Titolari e i Responsabili sulle misure di sicurezza da adottare al fine di garantire la tutela nel trattamento dei dati. Con l'eliminazione dell'allegato B del Codice del 2003 il Regolamento ha voluto che le misure di sicurezza fossero stabilite scientemente dal Titolare e/o dal Responsabile secondo le proprie esigenze, attraverso la valutazione dei rischi di sicurezza che i trattamenti comportano. Con tale abrogazione, infatti, il regolamento ha teso evitare adempimenti onerosi per quei Titolari che svolgevano trattamenti di dati personali limitati. L'art. 32 dedicato alla sicurezza del trattamento stabilisce quali siano le caratteristiche specifiche dei comportamenti che il Titolare e il Responsabile devono adottare affinché i dati personali vengano tutelati adeguatamente per garantire un livello di sicurezza proporzionato al rischio, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento. Nel valutare l'adeguamento, il Titolare e il Responsabile dovranno tener conto in special modo dei rischi del trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o abusivo, ai dati personali trasmessi, conservati o comunque trattati. Pertanto, sulla scorta del comma 4 del medesimo articolo, chiunque agisca sotto l'autorità del Titolare e/o del Responsabile e abbia accesso ai dati personali, non deve trattare tali dati se non opportunamente istruito da questi ultimi.

1.1 SCOPO DEL DOCUMENTO

Scopo del presente documento è descrivere il processo e le modalità operative adottate nel complesso di strutture facenti capo alla **Azienda Sanitaria Locale "Salerno"** (di seguito sinteticamente indicata come "ASL" "ASL Salerno" o "ASL di Salerno") per la gestione ed il controllo degli accessi logici ai sistemi Informatici, al fine di proteggere le risorse informative aziendali da accessi e trattamenti non autorizzati che avvengono attraverso strumenti elettronici.
Tale procedura si inquadra nell'insieme delle misure organizzative e procedurali disposte dal Titolare del trattamento, finalizzate all'indirizzamento e alla regolamentazione dei processi interni alla ASL di Salerno, dedicati alla gestione delle utenze, in ottemperanza al principio di responsabilizzazione ("*accountability*") del Titolare.

1.2 CAMPO DI APPLICAZIONE

In considerazione dell'elevata capillarità dell'ASL, a cui fanno capo ben 13 Distretti Sanitari e 12 Presidi Ospedalieri, è necessario valutare con la massima attenzione tale procedura. Il presente documento si riferisce, perciò, alle seguenti Unità Organizzative della ASL di Salerno:

- GRU (Gestione Risorse Umane)
- Responsabile di Servizio / Direttore della struttura complessa di riferimento
- SIA (Servizio Informativo Aziendale)
- Dipendenti e collaboratori esterni
- Gestore Esterno

29

1.3 RIFERIMENTI

Il presente paragrafo contiene la lista dei documenti di riferimento afferenti alla Struttura Sanitaria.

- Regolamento (UE) 679/2016 (GDPR)
- D. Lgs. 196/2003 così come novellato dal D. Lgs. 101/2018 recante disposizioni per l'adeguamento della normativa nazionale al Regolamento EU/679/2016
- ISO/IEC 27000
- Politica per gli amministratori di sistema
- Politica per l'utilizzo delle risorse informatiche

1.4 DEFINIZIONI

Termine	Descrizione
Account	Attributi di accesso di un utente su un sistema informatico, controllato in base ad un record di informazioni contenente almeno l'User-ID, la password ed i diritti/privilegi/restrizioni associati
Credenziali	L'insieme degli elementi identificativi di un utente o di un account
Macchina	Il supporto informatico messo a disposizione del dipendente contenente il software e/o in grado di collegarsi in rete per l'utilizzo dei sistemi informatici e degli applicativi della struttura
Password	Sequenza di caratteri alfanumerici e/o speciali tenuta segreta e necessaria per autenticarsi ad un sistema informatico o ad un applicativo
Credenziali "at least privilege"	Principio di sicurezza secondo il quale ad un utente viene concesso il privilegio minimo indispensabile che consente il livello di accesso necessario a svolgere le attività lavorative di sua competenza
Credenziali "need to Know"	Principio di sicurezza secondo il quale ciascun utente deve essere a conoscenza delle sole informazioni a lui necessarie per lo svolgimento delle sue attività lavorative
Credenziali "need to do"	Principio di sicurezza secondo il quale vengono concessi i profili di privilegio strettamente necessari per svolgere le attività lavorative di propria competenza
User ID	Sequenza alfanumerica che identifica univocamente (generalmente in associazione con una password) un utente ad un sistema
Utente	Qualunque soggetto autorizzato ed abilitato ad accedere a risorse informative o ad utilizzare servizi informatici aziendali
VPN	Virtual Private Network
AREAS	Sistema in uso presso ASL di Salerno per lo scambio e protocollo delle comunicazioni all'interno dell'Azienda Sanitaria Locale di Salerno
HD CED	Sistema di Help Desk attraverso cui vengono gestiti i ticket di assistenza
Ticket	Richiesta di assistenza tracciata dal sistema informatico di gestione in uso presso Asl di Salerno. A seconda della tipologia di richiesta viene indirizzata al gestore esterno o al SIA

Tabella 1 – Definizioni

30

2 OVERVIEW DEL PROCESSO

Il processo di creazione, emissione, modifica e cancellazione degli accessi logici ha come obiettivo quello di definire regole e meccanismi di abilitazione e restrizione che governino l'accesso, dall'interno e/o dall'esterno di un'organizzazione, ai dati, applicazioni e sistemi attraverso strumenti elettronici. Ciò al fine di stabilire e verificare una specifica gerarchia autorizzativa mediante l'insieme di misure di sicurezza di natura organizzativa, operativa e tecnologica.
Nel dettaglio il presente documento descrive le procedure che disciplinano la gestione delle utenze informatiche presso la ASL di Salerno per governare:

- La creazione di un'utenza;
- Il reset di un'utenza;
- La modifica dei privilegi dell'utenza;
- La disabilitazione di un'utenza;
- La revisione periodica delle utenze attive.

2.1 TIPOLOGIE DI UTENZE

Le utenze per l'accesso ai sistemi informatici, gestite secondo i processi descritti nel presente documento, sono raggruppabili nelle seguenti tipologie:

- **Utenze base**: utenze associate univocamente ad una persona fisica, abilitate per l'accesso agli strumenti informatici comuni ed agli apparati in generale. Fanno parte dell'utenza base, il dominio mail, il dominio per il controllo della posizione del dipendente nei confronti dell'azienda (buste paga, CUD, richiesta ferie e permessi) e l'accesso alla piattaforma applicativa per cui è stato autorizzato;
- **Utenze applicative**: utenze associate in maniera univoca ad una persona fisica, attraverso cui un soggetto è riconosciuto da un applicativo o da un programma ed è abilitato all'uso di funzioni applicative specifiche, legate al proprio ruolo all'interno della struttura complessa di cui fa parte.

Gli utenti, relativamente ai sistemi della struttura sanitaria sono suddivisi in classi:

- **User:** può accedere al sistema informatico ed al relativo database, se applicabile, può inserire nuove informazioni, modificare e salvare quelle già esistenti in base ai privilegi concessi dall'amministratore;
  - **Livelli:** le utenze User sono suddivise in diversi livelli a seconda della tipologia di privilegi di accesso assegnati per i diversi sistemi/applicazioni.
- **Power User:** può eseguire, oltre tutte le attività relative all'utente "User", controlli in sola lettura delle informazioni contenute nel patrimonio informativo, utilizzando funzionalità avanzate come il recupero dei record ad esso necessari per attività di verifica;
- **Administrator:** può eseguire, oltre tutte le attività relative agli utenti "User" e "Power User", le attività di assegnazione, modifica (ma non dei privilegi associati all'utenza) e reset delle utenze, resettare le macchine date in uso agli utenti, modificando o aggiungendo software e controllare i file di log degli utenti;
- **Super Administrator:** può eseguire, oltre tutte le attività relative all'utente "Administrator" anche le attività di assegnazione e modifica dei privilegi associate alle singole utenze attraverso apertura di ticket di assistenza.
- **Guest:** è il soggetto esterno che riceve una utenza "User" temporanea con la quale può accedere al sistema informatico in sola lettura. Non è autorizzato alla modifica dei record già esistenti.

31

2.2 RUOLI E RESPONSABILITÀ

RUOLO	RESPONSABILITÀ
Utente	Colui che ha la necessità di accedere ai sistemi informatici ed effettua il collegamento all'infrastruttura informatica attraverso le credenziali ottenute rispettando le politiche di sicurezza e le procedure della Asl di Salerno.
GRU	Ufficio Gestione Risorse Umane, si occupa della gestione amministrativa di tutti i dipendenti e di tutte le comunicazioni relative al rapporto tra questi e la Struttura Sanitaria.
Responsabile di Servizio	Colui che, in qualità di responsabile del soggetto esterno autorizzato / dipendente della Struttura Sanitaria, può richiedere la creazione dell'utenza a cui potranno corrispondere diversi privilegi in base alle esigenze lavorative. Allo stesso modo, il Responsabile di Servizio potrà richiedere la modifica dei privilegi o la disabilitazione dell'utenza.
Gestore Esterno	Si occupa della ricezione dei ticket relativi alle richieste di assistenza
SIA (Servizio Informativo Aziendale)	È l'insieme delle infrastrutture, delle procedure organizzative e delle risorse umane finalizzate alla gestione delle informazioni prodotte, utilizzate e condivise da un'azienda durante l'esecuzione dei processi aziendali. Si occupa materialmente di creare, modificare, resettare un'utenza e di gestire i profili attivi, disattivandoli quando necessario. Inoltre, si occupa del controllo periodico delle utenze.

Tabella 2 – Ruoli e Responsabilità

3 DESCRIZIONE DEL PROCESSO

Il processo si pone l'obiettivo di definire le modalità operative con cui le utenze devono essere gestite durante il loro intero ciclo di vita.
In particolare, definisce le seguenti fasi di governo delle utenze:

3.1 **Creazione dell'utenza**: in tale fase vengono descritte le operazioni necessarie all'attivazione di un'utenza ed il successivo rilascio delle opportune credenziali e privilegi di accesso;

3.2 **Reset dell'utenza**: in questa fase vengono descritte le attività di richiesta di reset dell'utenza tramite ticket e successive operazioni di invio delle nuove credenziali di accesso per i soli account impersonali e di servizio (i.e. password temporanea);

3.3 **Modifica dei privilegi dell'utenza**: in tale fase vengono descritte le attività di richiesta di modifica dei privilegi utente ed il rilascio degli stessi;

3.4 **Disabilitazione dei servizi sull'utenza**: in tale fase vengono descritte le attività necessarie alla disabilitazione dei servizi attivi sull'utenza nel momento in cui il soggetto utente non ha più necessità di utilizzarli (e.g. licenziamento, scadenza contratto, fine mandato etc.).

3.5 **Revisione periodica delle utenze attive**: in tale fase vengono verificate le condizioni che giustificano l'assegnazione delle utenze e della corrispondenza dei privilegi associati ai profili di accesso rilasciati.

33

Al fine di descrivere il processo, sono descritte le relative attività di tramite:

- una rappresentazione grafica dei flussi (flow-chart) che compongono il processo;
- una matrice che descrive analiticamente tale rappresentazione.

I simboli utilizzati nel flow-chart, con una breve descrizione degli stessi, sono illustrati nella seguente tabella:

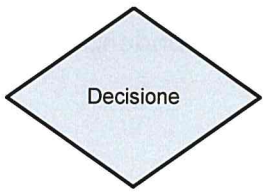
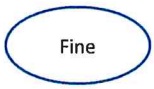
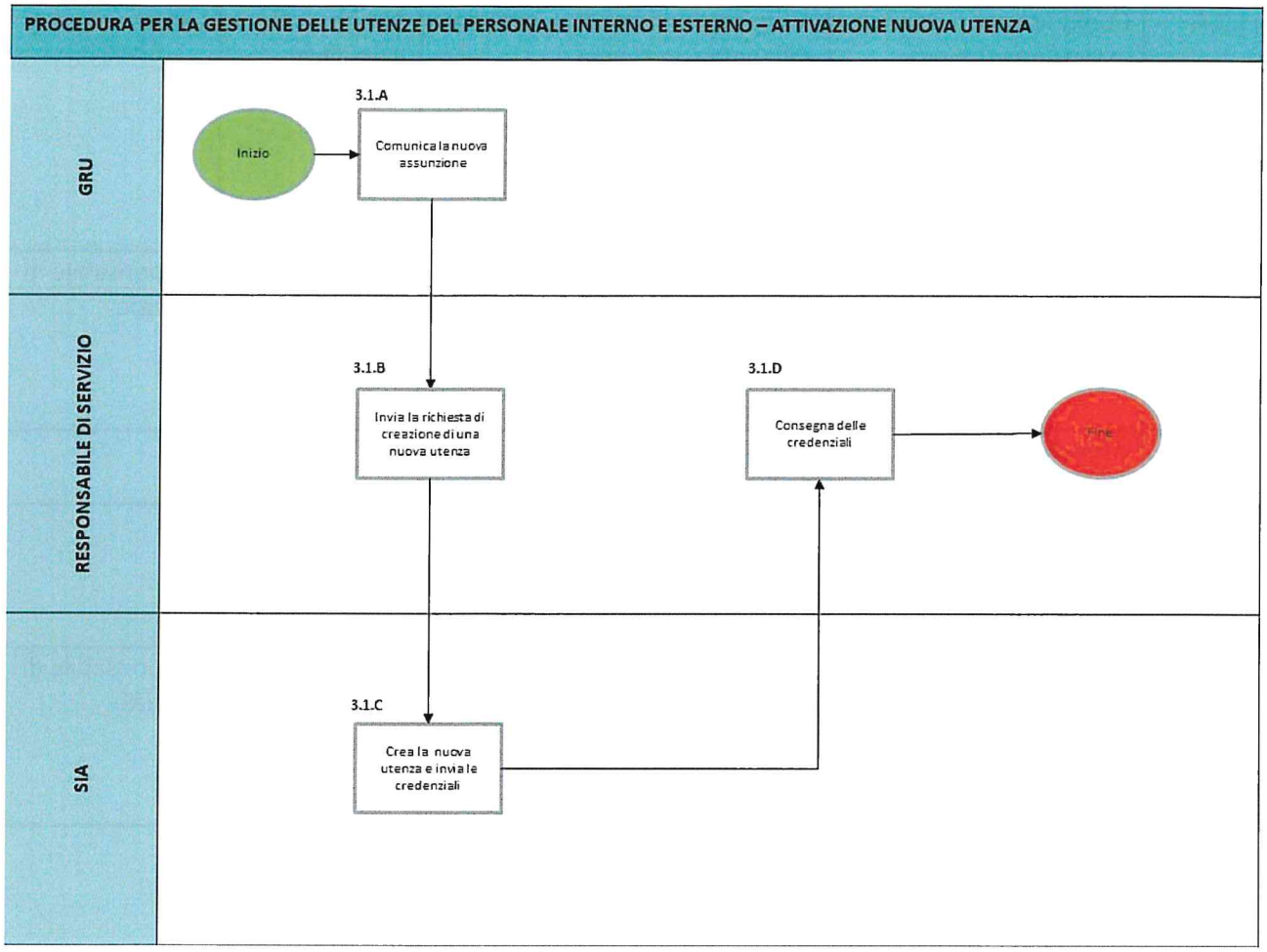
Simbolo	Denominazione	Descrizione
	Inizio	Rappresenta l'inizio del processo.
3.1.A 	Attività	Rappresenta la singola attività attuata, identificata da: • dal numero della Fase di riferimento • la lettera rappresenta l'attività seguita da una fase di decisione
	Decisione	Rappresenta un momento decisionale.
	Linee di flusso	Connette le attività fra di loro indicando il flusso delle informazioni.
	Fine	Rappresenta la fine del processo.

Tabella 3 – Legenda

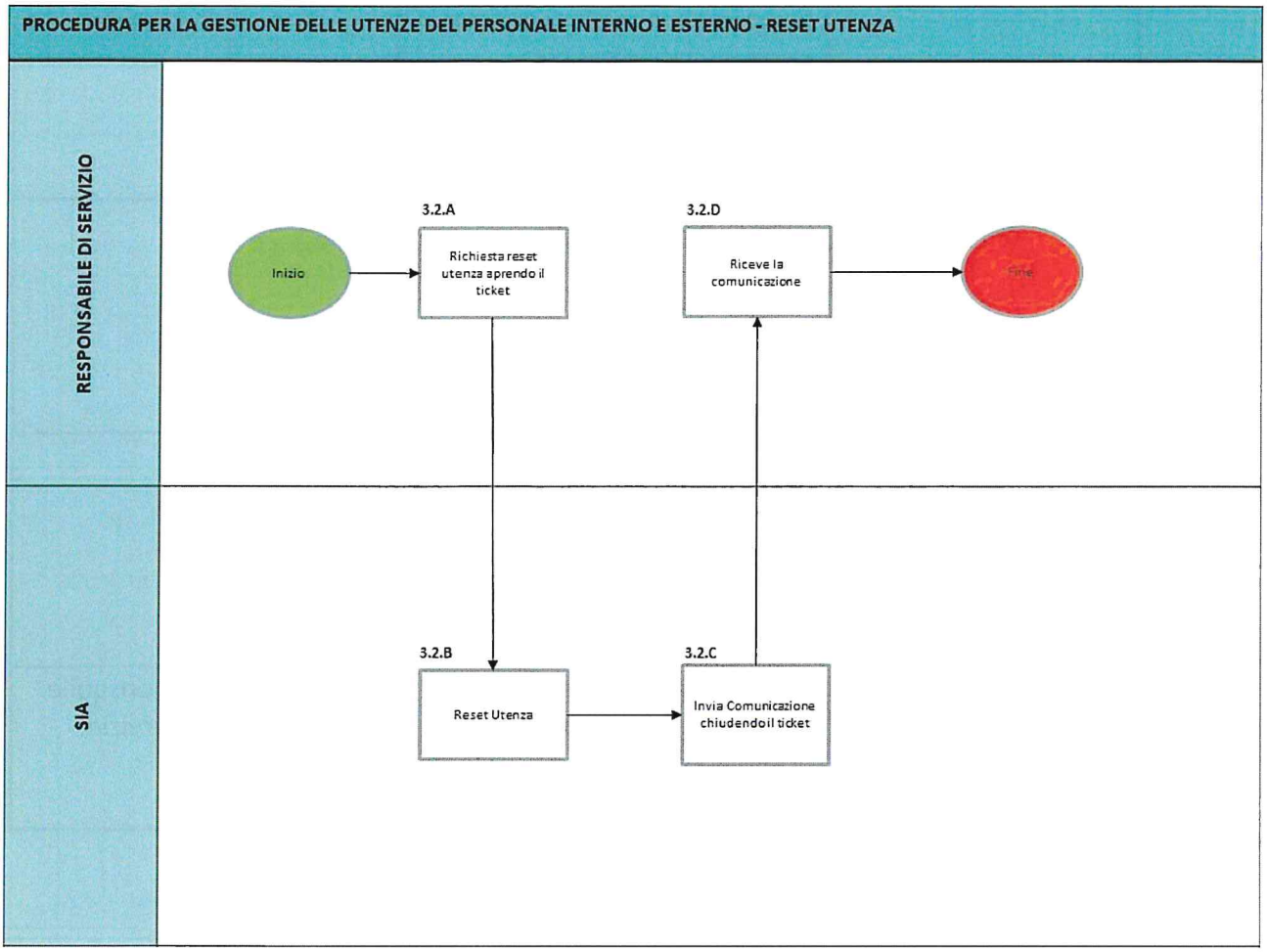
3.1 CREAZIONE DELL'UTENZA



ID	Attività	Descrizione	Strumento	Responsabilità
3.1.A	Comunicazione nuova assunzione / nuova collaborazione	A seguito di nuova assunzione o collaborazione viene predisposta la lettera di immissione in servizio che viene comunicata al Responsabile di Servizio dell'ufficio in cui sarà collocata la risorsa	AREAS Protocollo	GRU
3.1.B	Invio richiesta	Il Responsabile di Servizio, ricevuta la comunicazione, apre il ticket al SIA per la richiesta di attivazione di una nuova utenza con privilegi base	HD CED	Responsabile di Servizio
3.1.C	Attivazione utenza	Il SIA procede alla creazione dell'utenza con i privilegi base	N/A	SIA
3.1.D	Inoltro comunicazione	Il SIA inoltra la comunicazione di attivazione della nuova utenza al Responsabile di Servizio	HD CED	SIA
3.1.E	Consegna credenziali	Il Responsabile di Servizio consegna le credenziali (User id e password) all'utente. Quest'ultimo modificherà la password al primo accesso	*Brevi manu*	Responsabile di Servizio

Tabella 4 – Flow-chart e Matrice – Attivazione Utenza

3.2 RESET DELL'UTENZA



37

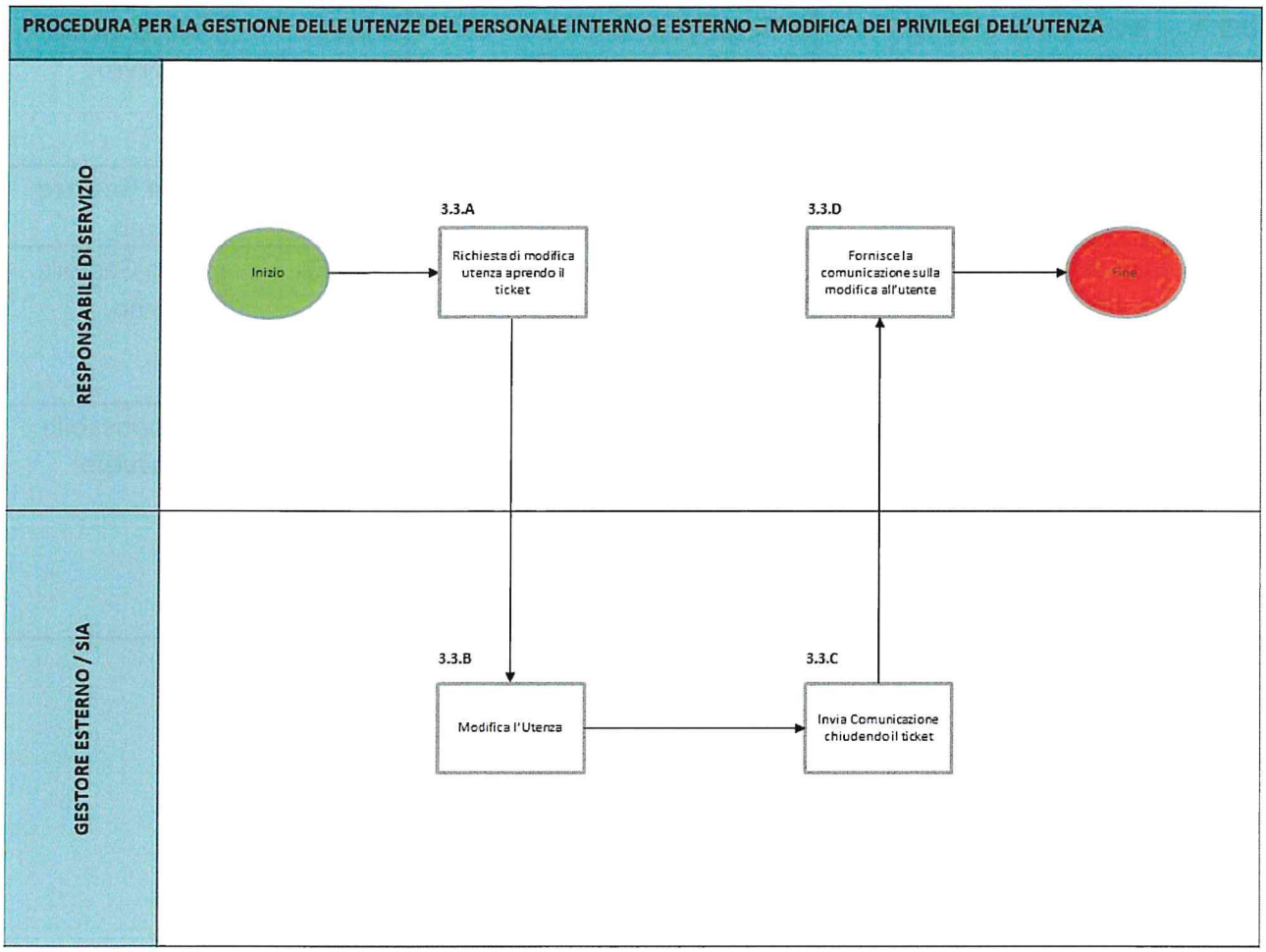
ID	Attività	Descrizione	Strumento	Responsabilità

3.2.A	Richiesta reset	Il Responsabile di Servizio invia la richiesta di reset dell'utenza aprendo il ticket al SIA	HD CED	Responsabile di Servizio
3.2.B	Reset utenza	Il SIA resetta l'utenza	N/A	SIA
3.2.C	Comunicazione reset	Il SIA comunica al Responsabile di Servizio l'avvenuto reset chiudendo il ticket	HD CED	SIA
3.2.D	Comunicazione all'utente	Il Responsabile di Servizio modificherà la password al primo accesso	N/A	Responsabile di Servizio

Tabella 5 – Flow-chart e Matrice – Reset Utenza

28

3.3 MODIFICA DEI PRIVILEGI SULL'UTENZA



39

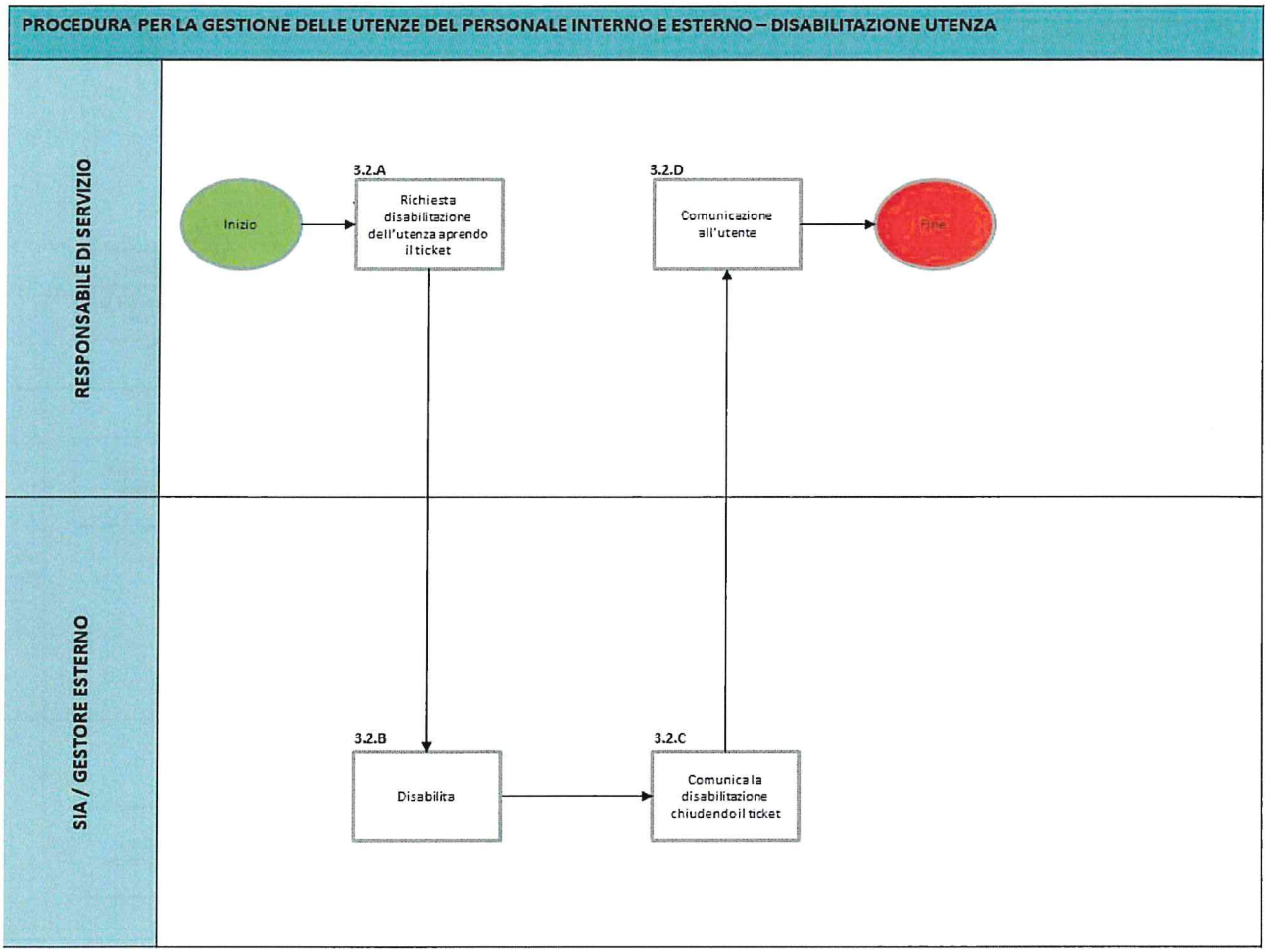
ID	Attività	Descrizione	Strumento	Responsabilità

3.3.A	Richiesta di modifica dell'utenza	Il Responsabile di Servizio richiede di modificare i privilegi associati ad un'utenza aprendo il ticket	HD CED	Responsabile di Servizio
3.3.B	Modifica Utenza	Il SIA o il Gestore Esterno modifica l'utenza	N/A	SIA o Gestore Esterno
3.3.C	Conferma della modifica e invio comunicazione	Il SIA o il Gestore Esterno invia la conferma di avvenuta modifica sull'utenza e chiude il ticket	HD CED	SIA o Gestore Esterno
3.3.D	Ricezione e conferma modifica	Il Responsabile di Servizio riceve la comunicazione e informa l'utente dell'avvenuta modifica inviando una copia della comunicazione al GRU	AREAS Protocollo	Responsabile di Servizio

Tabella 6 – Flow-chart e Matrice –Modifica dei privilegi Utenza

40

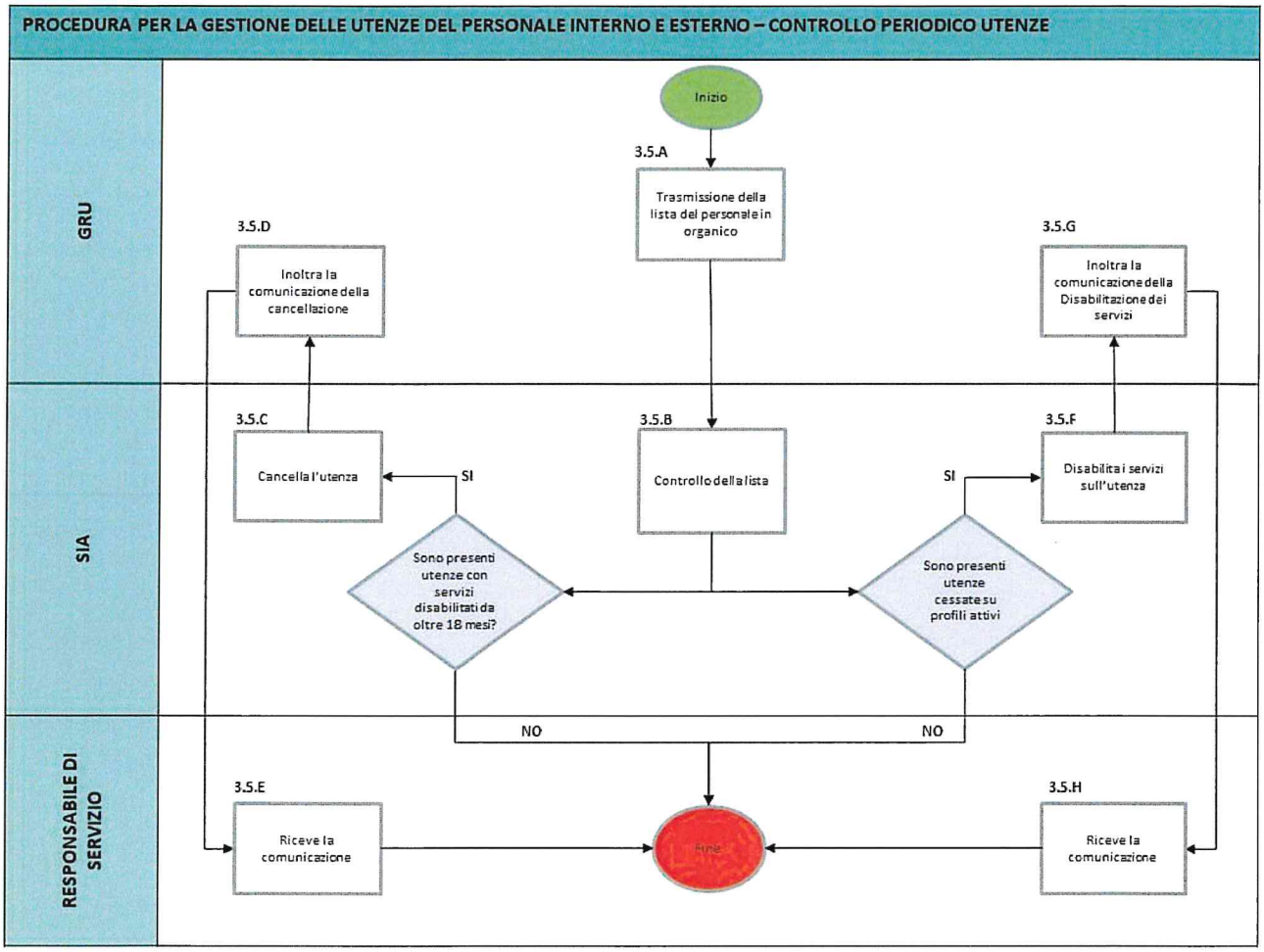
3.4 DISABILITAZIONE DELL'UTENZA



ID	Attività	Descrizione	Strumento	Responsabilità
3.4.A	Richiesta disabilitazione utenza	Il Responsabile di Servizio richiede la disabilitazione dell'utenza al SIA o al Gestore Esterno aprendo il ticket	HD CED	Responsabile di Servizio
3.4.B	Disabilitazione	Il SIA o il Gestore Esterno disabilita l'utenza	N/A	SIA o Gestore Esterno
3.4.C	Comunicazione di disabilitazione	Il SIA o il Gestore Esterno invia la comunicazione di disabilitazione al Responsabile di Servizio chiudendo il ticket	HD CED	SIA o Gestore Esterno
3.4.D	Comunicazione all'utente	Il Responsabile di Servizio comunica all'utente la disabilitazione dell'utenza	N/A	Responsabile di Servizio

Tabella 7 – Flow-chart e Matrice – Disabilitazione Utenza

3.5 REVISIONE PERIODICA DELLE UTENZE ATTIVE



42

ID	Attività	Descrizione	Strumento	Responsabilità
3.5.A	Trasmissione lista personale in organico	Il GRU trasmette **mensilmente** una lista del personale interno ed esterno in organico alla Struttura Sanitaria	AREAS Protocollo	GRU
3.5.B	Controllo sulle liste	Il SIA esegue il controllo sulla lista confrontandola con le utenze attive	N/A	SIA
3.5.C	Cancellazione utenza	Il SIA durante i controlli potrebbe tracciare delle utenze con servizi disabilitati. Se il periodo di disabilitazione supera i 18 mesi il SIA cancella l'utenza	N/A	SIA
3.5.D	Ricezione comunicazione di cancellazione	Il GRU riceve la comunicazione di cancellazione ed inoltra al Responsabile di Servizio	AREAS Protocollo	GRU
3.5.E	Ricezione comunicazione di cancellazione	Il Responsabile di Servizio riceve comunicazione di avvenuta cancellazione	AREAS Protocollo	Responsabile di Servizio
3.5.F	Disabilitazione utenza	Il SIA, eseguito il controllo sulla lista, riscontrando la presenza di un'utenza cessata non collegata ad un profilo attivo, disabilita tutti i servizi sull'utenza lasciando attivo su di essa il servizio per la consultazione dei documenti contabili relativi al rapporto di lavoro	N/A	SIA
3.5.G	Ricezione comunicazione di disabilitazione	Il GRU riceve la comunicazione di disabilitazione dei servizi sull'utenza, aggiorna la lista ed inoltra la comunicazione al Responsabile di Servizio	AREAS Protocollo	GRU
3.5.H	Ricezione comunicazione di disabilitazione	Il Responsabile di Servizio riceve comunicazione di avvenuta disabilitazione dei servizi sull'utenza	AREAS Protocollo	Responsabile di Servizio

Tabella 8 – Flow-chart e Matrice – Controllo periodico Utenze