REGIONE AUTONOMA FRIULI VENEZIA GIULIA

ente per la gestione accentrata dei servizi condivisi

EGAS

Gestione delle credenziali e dei profili di accesso

MATRICE DELLE REVISIONI					
REVISIONE	DATA	DESCRIZIONE / TIPO MODIFICA	REDATTA DA	VERIFICATA DA	APPROVATA DA
00	05/09/2017	Emissione	Servizio Informativo Carlo De Angelis Servizio Informativo Nicola Bortolotti	Direttore Amministrativo Tecla Del Do Direttore SC Economico Finanziaria Nives Di Marco Politiche e Gestione Risorse Umane Daniela Martini Affari Generali Alessandro Camarda, Sonia Borghese	Direttore Generale Massimo Romano
01	10/12/2018	Prima Revisione	Servizio Informativo Nicola Bortolotti	Direttore Amministrativo Tecla Del Do Direttore SC Economico Finanziaria Nives Di Marco Politiche e Gestione Risorse Umane Daniela Martini Affari Generali Alessandro Camarda, Sonia Borghese	Direttore Generale Massimo Romano
02					
03					
04					
05					

Approvato con decreto n. 122 del 27/12/2018

Indice

Scopo ed applicazione 4
Destinatari 4
Soggetti preposti alle richieste 4
Modalità operativa per la richiesta delle credenziali 5
Modalità di rilascio delle credenziali 5
Re-inizializzazione password 6
Revoca/Cessazione delle credenziali 6
Revisione delle credenziali 6
Profili di abilitazione 6
Riferimenti Normativi 6
Terminologia 7
Abbreviazioni 7

Scopo ed applicazione

Il presente documento ha lo scopo di definire i criteri per la creazione e l'utilizzo delle credenziali di autenticazione degli Incaricati dei servizi informatici e delle ulteriori strutture preposte dell'EGAS "Ente per la gestione accentrata dei servizi condivisi" di Udine - di seguito Azienda - UE 2016/679 "regolamento del parlamento europeo e del consiglio" relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e alle indicazioni ufficiali pubblicate da AgID per valutare ed innalzare il livello di sicurezza informatica delle PA in riferimento all'avvenuta pubblicazione in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».
La presente procedura richiama, in un separato documento che verrà implementato ed aggiornato dal Servizio Informativo, i profili di abilitazione dei singoli applicativi che possono essere attribuiti a ciascuna funzione/figura professionale presente in Azienda.
Il sistema di autenticazione per l'accesso ai servizi e agli applicativi consiste in un codice per l'identificazione dell'incaricato "user name" associato ad una parola chiave riservata "password", conosciuta esclusivamente dall'Incaricato: i due elementi costituiscono le credenziali di autenticazione o "account".
Lo user name viene assegnato e variato esclusivamente dall'amministratore di Sistema (interno o esterno all'Azienda), le utenze sono di tipo nominale e pertanto riconducibili al soggetto assegnatario. La password è gestita, dopo la prima assegnazione da parte dell'amministratore, esclusivamente dall'Incaricato, con l'eccezione dei casi in cui ricorrano necessità di carattere tecnico organizzative. Nemmeno il personale dei Sistemi Informatici ed il personale di Aziende Terze che per essi operano, hanno ragione alcuna di richiedere la password personale ad un Incaricato, che è tenuto ad adottare, nell'ambito delle proprie attività, tutte le misure di sicurezza atte a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche siano esse hardware che software.
Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice userid, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi.
È assolutamente vietata la detenzione abusiva, la diffusione e l'indebita appropriazione di credenziali di autenticazione.

Destinatari

Il documento è destinato a tutti i dipendenti e al personale autorizzato (di seguito "Incaricato") dell'Azienda.

Soggetti preposti alle richieste

Il solo personale autorizzato alla richiesta di nuove credenziali - e/o modifica e revoca delle stesse - è individuato nelle figure dei dirigenti delegati; essi hanno facoltà di istanziare richieste per il personale incardinato nella struttura amministrata.
L'eventuale delega, compilata secondo il modello predisposto, dovrà essere consegnata al Servizio Informativo con firma autografa in originale oppure sottoscritta digitalmente dal dirigente delegato ed inviata a mezzo IterAtti/GIFRA.
Nelle situazioni in cui il rilascio delle credenziali rappresenti carattere di "urgenza" ed il dirigente delegato risulti impossibilitato ad effettuare la richiesta, per esempio a seguito di

assenza, la modulistica potrà essere inoltrata dal superiore del dirigente delegato in maniera gerarchica (in ultimo dal Titolare stesso).

Modalità operativa per la richiesta delle credenziali

All'atto dell'assunzione, tutti gli Incaricati devono avere accesso alle risorse informatiche aziendali; è pertanto previsto, per tutti i Neo Assunti, il rilascio di un account per l'accesso al dominio e alla posta elettronica ordinaria (PEO). La struttura Politiche e Gestione Risorse Umane, comunica al Servizio Informativo l'assunzione della nuova risorsa indicando la data di fine rapporto per tutti i casi diversi dal tempo indeterminato. Ad evasione delle inerenti attività – creazione dell'utenza, della cassetta di posta istituzionale – il Servizio Informativo consegna la busta chiusa contente le credenziali personali alla struttura Politiche e Gestione Risorse Umane che le conserverà con la massima cura/riservatezza sino al momento di affidarle direttamente all'interessato durante la presa in servizio (consultare la relativa sezione MODALITÀ DI RILASCIO DELLE CREDENZIALI).
I dirigenti delegati possono richiedere per i propri collaboratori l'accesso agli applicativi utilizzati in Azienda. Contestualmente o in seguito alla produzione delle credenziali di accesso ai dispositivi (dominio), il dirigente delegato, procede all'invio della richiesta al Servizio Informativo per gli accessi ai servizi e agli applicativi disponibili.
Alla data di pubblicazione del presente documento, le credenziali vanno richieste utilizzando l'apposita modulistica liberamente accessibile sulla bacheca dello storage aziendale. La modulistica deve essere compilata in ogni sua parte e sottoscritta dal dirigente delegato prima di essere consegnata in originale al Servizio Informativo (ovvero inoltrata dalla PEO aziendale personale del dirigente delegato all'indirizzo servizio.informativo@egas.sanita.fvg.it).
La compilazione della richiesta in modalità non conforme a quanto indicato potrà comportare la sospensione della pratica.
Ogni struttura operativa è tenuta ad organizzare e conservare la tenuta di un registro delle credenziali le richieste per i propri collaboratori; in tal modo potranno essere correttamente istanziate eventuali richieste di modifica e cessazione.
È altresì dovere dei dirigenti delegati formalizzare la richiesta di revoca delle singole credenziali di accesso precedentemente assegnate ai propri collaboratori qualora vengano meno le condizioni per l'utilizzo delle credenziali stesse. L'attività di revoca viene gestita con la medesima modulistica preposta al rilascio di nuove credenziali.
Ad ogni Incaricato possono essere attribuite più credenziali di autenticazione (coppie username-password) in relazione all'applicativo, al ruolo e alle funzioni da svolgere.
Il medesimo username non può essere assegnato, neppure in tempi diversi, ad altri Incaricati.
Le parte riservata della credenziale (*password*), come previsto dalla normativa sulla privacy nell'ambito della gestione di dati personali e sanitari, deve essere modificata ogni 90 giorni.

Modalità di rilascio delle credenziali

L'Incaricato ritira personalmente presso la struttura Politiche e Gestione Risorse Umane le sole credenziali di accesso ai dispositivi (le medesime utilizzate per l'utilizzo della posta elettronica).
La busta conterrà:

- Le credenziali di autenticazione al dominio e alla posta elettronica;
- Le istruzioni per il cambio password al primo accesso;
- Le caratteristiche che deve avere una password (robusta) previste dalla normativa privacy;
- Le indicazioni circa la disponibilità dei regolamenti per l'utilizzo delle risorse informatiche.

Eventuali ulteriori credenziali di accesso agli applicativi, verranno inviate dagli amministratori dei sistemi direttamente alla cassetta e-mail personale (PEO) dell'Incaricato. Le credenziali saranno rilasciate in conformità a quanto previsto dalla vigente normativa, ossia separando la lettera cifrata dalla chiave di cifratura (codice da utilizzare per decifrare il contenuto).

Re-inizializzazione password

In caso di smarrimento o scadenza della password di accesso ai dispositivi (dominio) l'incaricato dovrà presentarsi - previo appuntamento e munito di documento di identità in corso di validità - presso il Servizio Informativo per procedere d'intesa con gli amministratori alla re-inizializzazione della parte privata della credenziale.
Per la re-inizializzazione di password non afferenti al dominio (per esempio applicativi SISSR) la procedura seguirà quanto indicato nel terzo paragrafo della sezione "MODALITÀ DI RILASCIO DELLE CREDENZIALI".

Revoca/Cessazione delle credenziali

In caso di estinzione del rapporto contrattuale con l'Incaricato, la Struttura Politiche e Gestione Risorse Umane invia tempestiva comunicazione a mezzo di posta elettronica al Servizio Informativo e questi provvede ad inibire l'accesso ai Servizi Informatici aziendali (dominio, posta elettronica e share di rete) entro tre giorni lavorativi dal ricevimento della comunicazione (o non appena ne venga a conoscenza).
È altresì cura del dirigente delegato dell'utente da disabilitare, compilare la modulistica ed inviarla al Servizio Informativo per la richiesta di cessazione delle credenziali di accesso ai singoli applicativi per i quali l'utente era stato abilitato.

Revisione delle credenziali

La revisione delle autorizzazioni degli Incaricati e dei diritti di accesso ai sistemi - profili per la rete, singoli applicativi, cartelle e directory, banche dati ecc. - deve essere periodicamente svolta, sulla base delle esigenze della Struttura e secondo la normativa vigente, da parte dei singoli dirigenti delegati.

Profili di abilitazione

I dirigenti delegati hanno facoltà di richiedere, per i propri collaboratori, l'accesso agli applicativi elencati nel documento "SISTEMI INFORMATICI E PROFILI DI AUTORIZZAZIONE" stabilendo preventivamente i ruoli strettamente necessari alle funzioni per cui sono incaricati (compatibilmente al livello di responsabilità e al contesto in cui operano); l'autorizzazione concessa deve rispettare il principio di pertinenza, l'istanza dovrà pertanto essere opportunamente misurata dal Soggetto richiedente.
Le abilitazioni per il personale "esterno" (personale dipendente di altri enti comandato a prestare servizio presso l'Azienda, personale in servizio presso l'Azienda mediante somministrazione di lavoro interinale, Personale Esterno in Regime Di Accordi/Progetti, Dipendenti/Liberi Professionisti che presentano attività per associazioni di volontariato, consulenti, ecc..), vengono valutate e richieste, caso per caso, dai singoli dirigenti delegati che se ne assumono le responsabilità di legge.

Riferimenti Normativi

- UE 2016/679 "regolamento del parlamento europeo e del consiglio" relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

- D.lgs 196/2003 “Codice in materia di protezione dei dati personali"
- D.lgs 101/2018 Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del 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, nonche’ alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018)
- Circolare 18 aprile 2017, n. 2/2017 - Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»
- CAD - D. lgs 82/2005 “Codice dell’Amministrazione Digitale” e ss.mm.ii

Terminologia

“account”: indica quell'insieme di funzionalità, strumenti e contenuti attribuiti ad un nome utente in determinati contesti operativi, spesso in siti web o per usufruire di determinati servizi su Internet;
"autenticazione informatica": l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
"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;
“hardware”: si indica la parte fisica di un computer, ovvero tutte quelle parti elettroniche, elettriche, meccaniche, magnetiche, ottiche che ne consentono il funzionamento (dette anche strumentario);
"incaricati": le persone fisiche autorizzate a compiere operazioni di trattamento dei dati dal Titolare o dal Dirigente delegato e ad accedere alle Risorse informatiche aziendali;
"parola chiave/password": componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
"profilo di autorizzazione": l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
“dirigente delegato”: i dirigenti dell’Ente, espressamente delegati dal titolare all’attuazione delle disposizioni in materia di trattamento dei dati;
“risorse informatiche aziendali”: qualsiasi combinazione di apparati tecnologici dell'Azienda e del Sistema informativo Socio Sanitario Regionale (SISSR), hardware o software, utilizzati per le comunicazioni elettroniche ed elaborazione dei dati;
"sistema di autorizzazione": l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
“software”: è l'informazione o le informazioni utilizzate da uno o più sistemi informatici e memorizzate su uno o più supporti informatici. Tali informazioni possono essere quindi rappresentate da uno o più programmi, oppure da uno o più dati, oppure da una combinazione delle due;
"strumenti elettronici": gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Abbreviazioni

EGAS: Ente per la Gestione Accentrata dei Servizi.