Unione Europea

Repubblica Italiana

Regione Siciliana
Assessorato Regionale dell'Economia
Autorità Regionale per l'Innovazione Tecnologica

POR FESR SICILIA 2014-2020

Servizio 1
Controllo e verifica sulla gestione e conduzione delle infrastrutture e dei sistemi informativi della Regione Siciliana

Politica Specifica
Gestione delle utenze

SOMMARIO

1 INTRODUZIONE

1.1 Scopo

Gli argomenti trattati nel presente documento, indirizzano un insieme di regole, applicabili alla *Regione Siciliana*, volte a definire il processo di creazione, assegnazione, utilizzo e gestione delle utenze abilitate ad accedere ai sistemi informatici, con particolare riguardo a quelli preposti al trattamento di dati personali.

Nei capitoli successivi sono pertanto definite le regole di base per la gestione delle seguenti tipologie di utenza:

- Personale dipendente della *Regione Siciliana*;
- Personale esterno che opera presso la *Regione Siciliana*;
- Personale esterno dedicato all'erogazione di servizi in outsourcing.

La necessità di fornire tali indirizzamenti deriva dalla consapevolezza dell'importanza rivestita dai sistemi informatici, ai fini del corretto espletamento della missione istituzionale.

A tali considerazioni, devono inoltre essere aggiunti gli obblighi di adempimento al Regolamento UE 679/2016 ed alle normative emanate dal Garante per la protezione dei dati personali (di seguito Garante Privacy o Garante) in materia di trattamento dei dati sanitari e gestione degli amministratori di sistema [DR-1][DR-3].

Le politiche descritte all'interno del presente documento sono da considerarsi misure minime la cui attuazione si rende necessaria per contenere, entro limiti accettabili, il rischio di compromissioni della riservatezza, integrità e disponibilità delle risorse informative, derivanti da accessi impropri e/o non autorizzati.

In tal senso, queste costituiscono i requisiti di base che devono essere rispettati e che, in quanto tali, in virtù delle specifiche caratteristiche del contesto operativo cui si applicano, possono essere incrementati nei casi in cui siano richiesti livelli di protezione più elevati.

1.2 Ambito di Applicabilità

Le politiche descritte nel presente documento, si applicano a tutte le tipologie di utenze e a tutti i sistemi informativi della *Regione Siciliana*.

Le politichedi seguito descritte sono in vigore a partire dalla data di emissione del presente documento.

2 RIFERIMENTI

2.1 Documenti Applicabili

Rif.	Codice	Titolo
DA-1.	--	Capitolato Tecnico – Parte Generale "Procedura ristretta, suddivisa in 4 lotti, per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)"
DA-2.	--	Capitolato Tecnico – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)"
DA-3.	--	Offerta Tecnica – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (IS SIGEF 1403)" del 22 Dicembre 2014
DA-4.	--	Contratto Quadro Consip Lotto 2 "Servizi di gestione delle identità digitali e sicurezza applicativa

Tabella 1 - Documenti Applicabili

2.2 Documenti di Riferimento

Rif.	Codice	Titolo
DR-1.	--	Regolamento UE n. 679/2016 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE – General Data Protection Regulation (GDPR).
DR-2.	--	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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
DR-3.	--	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – Garante per la protezione dei dati personali – Provvedimenti a carattere generale – 27/11/2008 e succ. modificazioni.
DR-4.	--	Legge n.547 del 23 dicembre 1993 sul tema della criminalità informatica.
DR-5.	--	Codice penale dello Stato italiano.
DR-6.	--	Politica per la gestione degli amministratori di sistema– Regione Siciliana.

Tabella 2 - Documenti di Riferimento

3 DEFINIZIONI E ACRONIMI

3.1 Definizioni

Vocabolo	Titolo
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.
Amministratore di Sistema	È il soggetto, appositamente designato con provvedimento formale della *Regione Siciliana*, alla gestione e/o alla manutenzione dei sistemi informativi gestiti dalla medesima regione, ai sensi del provvedimento del Garante Privacy del 27 novembre 2008.
Credenziali	L'insieme degli elementi identificativi di un utente o di un account.
Credenziali "atleastprivilege"	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.
Password	Sequenza di caratteri alfanumerici e/o speciali tenuta segreta e necessaria per autenticarsi ad un sistema informatico o ad un applicativo.
Supporto Informatico	Il Supporto Informatico è il Computer o lo strumento elettronico messo a disposizione del dipendente contenente software ed in grado di collegarsi in rete per l'utilizzo dei sistemi informatici e degli applicativi della struttura.
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.
Utenze Amministrative	Utenze assegnate agli Amministratori di Sistema con riferimento al Provv. del Garante Privacy del 27 /11/2008 e s.m.i.
Utenze Amministrative Impersonali	Utenze amministrative impersonali utilizzate per l'amministrazione dei sistemi (es. root, administrator) con diritti di accesso privilegiati
Utenze tecniche (o di servizio)	Utenze tecniche impersonali presenti nel codice applicativo o nei server applicativi con diritti di accesso privilegiati

Tabella 3 - Definizioni

3.2 Acronimi

Codice	Titolo
Amministrazione	CONSIP
CE	Contratto Esecutivo
Committente	CONSIP
CQ	Contratto Quadro
GDPR	General Data Protection Regulation

Codice	Titolo
Raggruppamento	Raggruppamento Temporaneo di Impresa Leonardo Divisione Cyber Security S.p.A. (nel seguito Leonardo), società mandataria, IBMS.p.A. (mandante), Sistemi Informativi S.p.A. (mandante) e FastwebS.p.A. (mandante).
RTI	Raggruppamento Temporaneo di Impresa

Tabella 4-Acronimi

4 ETICA E COMPORTAMENTI SANZIONATI DALLE NORMATIVE VIGENTI

Tutto il personale abilitato ad accedere alle risorse informative deve essere consapevole che l'attuazione di alcuni comportamenti negligenti o non conformi alle politiche interne, oltre a non configurarsi come eticamente corretto, rappresenta anche un illecito e come tale perseguibile nell'ambito dell'ordinamento giuridico italiano.

Nello specifico contesto della presente Politica, costituisce un reato la messa in atto di determinati comportamenti configurabili come "crimini informatici", in particolare:

- L'accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- La detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.).

In caso di accertate violazioni delle norme sopra indicate si potrà provvedere all'immediata inibizione dell'account, fermo restando ogni valutazione di carattere disciplinare. A tale proposito si rimanda alla Legge n.547 del 23 dicembre 1993 [DR-4] e a tutte le successive modifiche, integrazioni e nuove Leggi emanate in materia.

5 ACCESSO ALLE RISORSE INFORMATICHE

Le norme d'uso adottate dalla *Regione Siciliana* per la regolamentazione delle utenze abilitate ad accedere alle risorse informatiche, rientrano nell'insieme delle misure di carattere organizzativo e procedurale disposte dal Titolare[1] del trattamento dei dati personali, in adempimento agli indirizzamenti di legge definiti dal Regolamento UE 679/2016 [DR-1].

Le credenziali assegnate a ciascun utente per l'accesso alle risorse informatiche (es. UserID, password), sono di uso strettamente personale e pertanto l'assegnatario è tenuto a custodirle con diligenza e in modo appropriato, al fine di contenere i rischi di accessi non autorizzati, furti, frodi, danneggiamenti derivanti dalla diffusione e/o utilizzo improprio delle credenziali utente (user account).

Gli utenti, hanno diritto di accesso limitato alle risorse informatiche per le quali sono stati espressamente autorizzati, e per gli utilizzi strettamente correlati con le mansioni assegnate.

Le credenziali utente devono avere carattere nominativo ed essere riconducibili ad una persona fisica. Tuttavia, le utenze afferenti a processi macchina utilizzate dai programmi informatici (utenze tecniche o di servizio), per le quali occorre definire requisiti e misure di sicurezza specifiche, possono avere carattere impersonale ma devono essere comunque riconducibili ad una persona fisica che ne è responsabile.

È previsto che gli Amministratori di Sistema accedano localmente ai sistemi informatici della *Regione Siciliana* (es. attraverso una console di sistema), utilizzando utenze amministrative impersonali (es, root, admin), nei seguenti casi eccezionali:

- Quando non sia disponibile la connettività di rete per l'accesso da remoto ai sistemi informatici da parte degli Amministratori di Sistema mediante le proprie utenze nominali;
- Per esigenze legate alla manutenzione ordinaria o straordinaria dei sistemi informatici da parte degli Amministratori di Sistema, laddove non sia possibile effettuare tali attività da remoto, utilizzando le proprie utenze nominali.

L'accesso locale (da console) ai sistemi informatici da parte degli Amministratori di Sistema attraverso utenze impersonali, nei casi eccezionali precedentemente indicati, è subordinato all'adozione di idonee procedure di emergenza atte ad assicurare:

- L'identificazione certa, anche fisica, dell'Amministratore di Sistema che andrà ad utilizzare l'utenza impersonale;
- Le motivazioni giustificative e lo scopo delle attività che richiedono l'uso dell'utenza impersonale;
- La registrazione della data e dell'ora di accesso e l'individuazione univoca del sistema/i interessato/i;
- La registrazione dell'intervallo di tempo (login-logout) durante il quale l'Amministratore di Sistema ha utilizzato l'utenza impersonale;
- Adeguata custodita delle password associate alle utenze impersonali, volta a garantirne la riservatezza e contestualmente la disponibilità nel momento in cui vi sia la necessità di utilizzarle;
- Validità temporanea della password utilizzata per l'accesso, limitata ad una singola sessione di intervento.

Nel caso in cui non siano previsti ambienti separati per il collaudo e l'esercizio dei sistemi informativi, tutte le utenze utilizzate per le attività di collaudo, devono essere rimosse prima del rilascio in esercizio di tali sistemi.

[1] Nella *Regione Siciliana*, a norma dello Statuto, il *Presidente* e gli *Assessori regionali* svolgono le funzioni esecutive ed amministrative e pertanto sono stati identificati come Titolari dei trattamenti dei dati personali di loro competenza (V. art. 20 dello Statuto della *Regione Siciliana*, parere dell'Ufficio Legislativo e Legale n. 132 del 2004 e n. 46 del 2005).

6 GESTIONE DELLE CREDENZIALI DI ACCESSO

Per accedere alle risorse informatiche della *Regione Siciliana*, ogni Utente deve possedere una credenziale di autenticazione (user account).

L'account è strettamente personale e non ne è ammesso l'utilizzo da parte di persone diverse dal legittimo proprietario, né questi può cederlo a terzi. L'Utente è responsabile di tutte le operazioni effettuate tramite il proprio account sui sistemi informatici.

Le credenziali di autenticazione, laddove utilizzate, non possono essere assegnate ad una persona fisica diversa dal primo assegnatario, neppure in tempi diversi.

La credenziale di autenticazione è composta come minimo da una UserId e da una password personale. La gestione delle credenziali di autenticazione è soggetta alle regole descritte nei paragrafi successivi.

6.1 UserId Policy

Lo UserId è univoco e deve essere sempre associato ad una sola persona fisica.

Nel momento in cui l'utente non ha più diritto/necessità di accedere ai sistemi informatici, lo userid deve essere disattivatoe non cancellato, al fine di consentire indagini future e/o di non riassegnarla a persone diverse anche in momenti diversi.

6.2 Password Policy

Di seguito vengono descritte le regole generali per la creazione e la gestione delle password per tutti gli utenti, a prescindere dagli eventuali ulteriori controlli e/o meccanismi specifici implementati in determinati contesti.

6.2.1 Regole semantiche per la creazione della password

La lunghezza minima delle password è stabilita in otto caratteri, sono ovviamente esclusi da tale regola i sistemi che non gestiscano questa lunghezza, per i quali si applicherà la lunghezza massima consentita.

Per gli Amministratori di Sistema la password deve essere costituita da almeno quattordici caratteri ovvero deve essere utilizzata una autenticazione forte.

Le password devono essere costruite utilizzando caratteri alfabetici, numerici e simboli speciali disponibili con le tastiere di utilizzo comune.

Le password devono contenere almeno un carattere alfabetico maiuscolo, un numero ed un carattere speciale.

Inoltre, non è consentito usare una password che:

- sia riconducibile ad un nome proprio di persona o derivante dallo userId (ad es. identico, inverso, con le lettere raddoppiate, ecc.) o comunque agevolmente riconducibile all'intestatario dello userId (ad es. matricola, cognome, dati anagrafici, ufficio/funzione di appartenenza);
- sia composta di sole cifre o di una lettera o carattere ripetuto anche più volte o ancora digitata attraverso l'uso della sola barra spaziatrice;
- contenga riferimenti a dati personali (ad es. indirizzo, telefono, codice fiscale, numero della patente, ecc.) o comunque ad altre parole agevolmente riconducibili all'utente;
- possano essere lette sia nell'uno che nell'altro verso (ad es. parole o frasi palindrome: ad es. adda, ossesso, esse, ingegni, ecc.);
- sia uguale alle ultime cinque utilizzate o uguale alla precedente tranne che per un carattere.

Qualora tecnicamente possibile, è necessario attivare i meccanismi di controllo automatico sulla generazione di password sicure eventualmente disponibili da sistema.

6.2.2 Regole per la gestione del ciclo di vita delle password

Di seguito sono esposte le regole relative a ciascuna fase del ciclo di vita della password.

Gli eventi che caratterizzano il ciclo di vita di una password possono essere così sintetizzati:

- **Generazione**: automatica o ad opera della funzione preposta;
- **Custodia**: ad opera del sistema e del legittimo proprietario (titolare);
- **Utilizzo**: ad opera del titolare;
- **Scadenza**: automatica per decorrenza del periodo di validità;
- **Modifica**: ad opera del titolare;
- **Blocco**: automatico o ad opera della funzione preposta.

6.2.2.1 Generazione

La generazione della prima password deve essere effettuata, dalla funzione preposta all'amministrazione degli account, in concomitanza con l'attivazione dell'identificativo utente (userId) ad essa correlato.

Nella generazione della prima password, devono essere utilizzate le regole esposte al paragrafo 6.2.1.

La prima password ha carattere provvisorio e qualora tecnicamente possibile, non attivaalcuna operazione diversa da quelle strettamente necessarie alla sua modifica da parte del titolare, con una nuova password conforme alle regole esposte nel paragrafo 6.2.1. Laddove non sia tecnicamente possibile forzare il cambio password in maniera automatica, il titolare è comunque tenuto ad effettuare il cambio password al primo accesso.

Nel caso in cuila prima password non possa essere tecnicamente modificabile dal titolare, ma esclusivamente dalla funzione preposta all'amministrazione degli account, occorrerà adottare le opportune misure compensative atte a garantire la segretezza della password assegnata al titolare.

6.2.2.2 Custodia

La password di accesso, relativa ad un determinato utente è strettamente personale e non può essere comunicata ad altri, anche se limitatamente a brevi periodi di utilizzo.

Le password devono essere conservate all'interno del sistema, in formato non intelligibile, utilizzando algoritmi hash standard sufficientemente robusti per garantire la non reversibilità della codifica. Non è ammessa in alcun caso la custodia in chiaro delle password.

Non è inoltre consentito:

- Comunicare la password (anche se scaduta) per telefono o altro mezzo a soggetti non autorizzati che si presentano come colleghi, tecnici, supervisori, autorità competenti, ecc.;
- Digitare la password davanti ad altri (ad es. colleghi o estranei) anche se si tratta del personale di assistenza tecnica;
- Trascrivere la password su dispositivi o supporti cartacei o elettronici (ad es. foglietti apposti sul personal computer, lasciati sulla scrivania o dentro ad un cassetto, file di testo lasciati sul desktop, ecc.). Qualora si rendesse indispensabile una trascrizione di back-up, questa dovrà essere custodita in apposito mezzo forte ad accesso limitato, ed il processo dovrà essere corredato da apposita procedura operativa che ne descriva il flusso di gestione, nonché le relative competenze e le responsabilità.

Infine, qualora si avesse anche solo il dubbio che la propria password sia venuta a conoscenza di altri è fatto obbligo al legittimo titolare di provvedere immediatamente a modificarla password e, nei casi più gravi, a segnalare la sospetta o accertata violazione alla funzione competente.

6.2.2.3 Utilizzo

Non è consentito che due o più persone fisiche accedano al sistema, simultaneamente o in maniera differita, utilizzando il medesimo identificativo utente.

6.2.2.4 Scadenza

Il periodo massimo di validità della password è stabilito in 90 giorni. Trascorso tale periodo, deve essere immediatamente attuata la procedura di modifica dellapassword oppure in assenza di tale funzionalità automatica, deve esserne disposto il blocco forzato da parte dalla funzione preposta all'amministrazione degli account, fino al compimento delle operazioni di cambio password.

6.2.2.5 Modifica

La modifica di una password è consentita esclusivamente al titolare. Il titolare modifica la propria password previo inserimento del proprio identificativo utente e della vecchia password.

Nella sostituzione della password, non può essere riutilizzata alcuna delle ultime 3 password di cui si è fatto precedentemente uso.

È vietata la sostituzione di una password con una frequenza superiore alle 2 volte al giorno in quanto tale evento potrebbe attivare controlli su presunte violazioni di sicurezza.

Il titolare deve effettuare la sostituzione della password provvisoria attribuitagli dalla funzione preposta all'amministrazione degli account in sede di attivazione o riattivazione dell'account, nel più breve tempo possibile.

Nel caso in cui la passwordnon possa essere tecnicamente modificabile dal titolare, ma esclusivamente dalla funzione preposta all'amministrazione degli account, occorrerà adottare le opportune misure compensative atte a garantire la modifica della password assegnata al titolare e la relativa segretezza.

6.2.2.6 Blocco

Per blocco si intende la sospensione temporanea di una utenza titolare, in maniera tale che non sia possibile effettuare sessioni di identificazione ed autenticazione (login) con quelle credenziali.

Il blocco dell'utenza deve essere effettuato ogni qualvolta si ipotizzi un rischio di accessi illeciti o di compromissione della password, e comunque ogni volta sia necessario per garantire la sicurezza sistema.

La procedura di blocco dell'utenza deve essere possibile solo da parte di un Amministratore di Sistema dotato di specifici privilegi di accesso.

6.3 Database delle utenze

Deve essere predisposto un archivio delle Utenze aventi accesso ai sistemi informativi della *Regione Siciliana*, su un supporto elettronico dedicato.

A valle della creazione e della modifica di tali utenze, da parte degli Amministratori, dovrà essere conseguentemente aggiornato il relativo archivio (registro delle utenze), con il dettaglio di tutte le operazioni su queste svolte (es. creazione, modifica, disattivazione).

L'accesso al registro delle utenze deve essere consentito esclusivamente al personale autorizzato.

6.4 Disattivazione automatica delle credenziali

Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica (es. Utenze tecniche o di servizio e Utenze Amministrative), per le quali devono essere predisposte specifiche procedure operative.

6.5 Principi per l'assegnazione dei profili autorizzativi

Per Profilo Autorizzativo (o privilegio utente), si intende un insieme di regole, relativo ad un applicazione/servizio, che ne definiscono le modalità di utilizzo da parte degli Utenti. Queste regole possono essere espresse nell'insieme di risorse ed attributi (c.d ruoli applicativi - Amministratore, Utente, Operatore) che ne regolano l'accesso.

I profili autorizzativi devono essere:

- Definiti sulla base delle specifiche applicazioni informatiche (es. sistemi, apparati di rete) che gli utenti devono utilizzare durante la normale attività lavorativa;
- In ragione del ruolo ricoperto e limitatamente alle mansioni svolte;
- Configurati per limitare l'accesso ai soli dati necessari alle finalità dell'attività lavorativa (principi del "*atleastprivilege*" e "*need to know*");
- Limitate nel tempo in ragione delle effettive necessità lavorative.

Il rilascio dei profili autorizzativi deve avvenire attraverso procedure formalizzate. Le procedure devono comprendere il rilascio delle autorizzazioni speciali per il personale tecnico-sistemistico, e di quelle eventualmente temporanee per il personale addetto alle assistenze/manutenzioni.

6.6 Verifica periodica delle Utenze e delle relative autorizzazioni

Al fine di ridurre le opportunità di modifica o di uso improprio e/o non autorizzato dei dati e delle informazioni trattate dalla *Regione Siciliana*, devono essere previste procedure formalizzate per la verifica periodica e comunque annuale, della sussistenza delle condizioni per il mantenimento dei profili autorizzativi, con particolare attenzione ai profili autorizzativi privilegiati (es. Amministratori di sistema).

I fattori che possono determinare un cambiamento nella definizione dei profili autorizzativi sono generalmente legati alle seguenti circostanze:

- Cambio di ruolo o mutamento delle mansioni svolte dal titolare dell'utenza;
- Mutamenti dello scenario tecnologico dell'infrastruttura informatica;
- Evoluzione dello scenario normativo di riferimento.