Unione Europea

Repubblica Italiana

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

FESR SICILIA 2014-2020

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

Prot. 4535 *Palermo,* 27/06/2022

OGGETTO: Trasmissione politiche specifiche per il corretto utilizzo delle risorse informatiche aziendali.

Allegati:

Nota inviata esclusivamente via email

Ai Capi di Gabinetto
Ai Dirigenti Generali
Ai Responsabili degli Uffici Equiparati
Ai Responsabili degli Uffici Speciali
Al Responsabile della Protezione dei dati (DPO)
Ai Referenti Informatici
Ai Referenti Privacy

Presidenza della Regione
Ufficio del Garante per la tutela dei diritti fondamentali dei detenuti

Ufficio della Presidenza
Autorità di Certificazione dei Programmi cofinanziati dallaCommissione Europea

Ufficio Speciale Autorità di Audit dei Programmi cofinanziati dalla Commissione Europea

Dipartimenti della Presidenza
Segreteria generale

Ufficio Legislativo e Legale

Dipartimento della Protezione Civile

Dipartimento della Programmazione

Dipartimento degli Affari Extraregionali

Autorità di Bacino del Distretto Idrografico della Sicilia

Uffici alle Dirette Dipendenze del Presidente
Ufficio stampa e documentazione

Ufficio di Rappresentanza e del Cerimoniale

Ufficio della Segreteria di Giunta

Ufficio di Bruxelles

Assessorato Attività Produttive
Ufficio di diretta collaborazione con l'Assessore

Dipartimento delle Attività Produttive

Assessorato Beni Culturali e identità Siciliana
Ufficio di diretta collaborazione con l'Assessore

Dipartimento dei Beni Culturali e dell'Identità Siciliana

Assessorato dell'Economia
Ufficio di diretta collaborazione con l'Assessore

Dipartimento del Bilancio e del Tesoro-Ragioneria

Dipartimento finanze e credito

Autorità Regionale per l'Innovazione tecnologica

Assessorato dell'Energia e Servizi di Pubblica Utilità
Dipartimento dell'Energia

Dipartimento dell'Acqua e dei Rifiuti

Assessorato alla Famiglia, Politiche Sociali e del Lavoro
Ufficio di diretta collaborazione con l'Assessore

Dipartimento della Famiglia e delle Politiche Sociali

Dipartimento del Lavoro, dell'Impiego, dell'Orientamento, dei Servizi e delle Attività Formative

Ufficio Speciale Immigrazione

Assessorato delle Autonomie Locali e Funzione Pubblica
Ufficio di diretta collaborazione con l'Assessore

Dipartimento della Funzione Pubblica e del Personale

Dipartimento delle Autonomie Locali

Assessorato delle Infrastrutture, Trasporti e Mobilità
Ufficio di diretta collaborazione con l'Assessore

Dipartimento delle Infrastrutture, della Mobilità e dei Trasporti

Dipartimento Regionale Tecnico

Assessorato dell'Istruzione e Formazione Professionale
Ufficio di diretta collaborazione con l'Assessore

Dipartimento della Formazione Professionale

Dipartimento dell'Istruzione e del diritto allo studio

Assessorato dell'Agricoltura, Sviluppo rurale e Pesca mediterranea
Ufficio di diretta collaborazione con l'Assessore

Dipartimento dell'Agricoltura

Dipartimento della Pesca Mediterranea

Dipartimento Sviluppo Rurale e Territoriale

Assessorato della Salute
Ufficio di diretta collaborazione con l'Assessore

Dipartimento per la Pianificazione Strategica

Dipartimento per le Attività Sanitarie e Osservatorio Epidemiologico

Assessorato Territorio e Ambiente
Ufficio di diretta collaborazione con l'Assessore

Dipartimento dell'Ambiente

Dipartimento dell'Urbanistica

Comando del Corpo Forestale della Regione siciliana

Assessorato Turismo, Sport e Spettacolo
Ufficio di diretta collaborazione con l'Assessore

Dipartimento del Turismo, dello Sport e dello Spettacolo

In conformità a quanto disposto nel codice di comportamento del personale dipendente della Pubblica Amministrazione (DPR n.63 del 16 aprile 2013), i rapporti ed i comportamenti, a tutti i livelli gerarchici, sono improntati a principi di diligenza,lealtà,imparzialità e buona condotta. Tali principi vengono applicati anche alle regole interne per la tutela della sicurezza delle risorse informatiche.

Il documento allegato definisce l'insieme di misure minime per l'accesso e l'utilizzo delle risorse informatiche della Regione Siciliana, la cui osservanza contribuisce a ridurre i rischi di violazioni della sicurezza informatica derivanti da una condotta non idonea da parte del personale interno e/o dei consulenti esterni e/o di terze parti che concorrono a vario titolo alla gestione dei processi posti sotto la responsabilità della Regione Siciliana, consapevoli che le risorse informatiche sono assegnate per esclusive finalità lavorative, e per perseguire scopi istituzionali della Regione Siciliana e che costituiscono un bene da custodire e tutelare.

Pertanto la finalità delle indicazioni/raccomandazioni formulate, nel documento allegato,dovranno essere rivolte e diffuse a tutti i dipendenti e/o collaboratori della Regione Siciliana, che forniscono le proprie prestazioni lavorative a qualsiasi titolo e sotto qualsiasi forma contrattuale, compresi tutti i soggetti che accedono ai sistemi informatici della Regione Siciliana nonché i visitatori e gli ospiti occasionali.

Il Dirigente del Servizio
(Giovanni Corrao)

Documento firmato da:
GIOVANNI CORRAO
27.06.2022 15:31:45 UTC

IlDirigente Generale
(*Vincenzo Falgares*)

VINCENZO FALGARES
Firmato digitalmente da VINCENZO FALGARES
Data: 2022.06.27 18:19:00 +02'00'

Unione Europea

Repubblica Italiana

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

FESR SICILIA 2014-2020

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

Politica Specifica
Corretto utilizzo delle risorse informatiche aziendali

Documento firmato da:
GIOVANNI CORRAO
27.06.2022 16:10:07 UTC

VINCENZO FALGARES
Firmato digitalmente da VINCENZO FALGARES
Data: 2022.06.27 18:15:37 +02'00'

SOMMARIO

LISTA DELLE TABELLE

1 INTRODUZIONE

1.1 Scopo

La presente politicadefinisce l'insieme delle regole per l'accesso e l'utilizzo delle risorse informatiche della *Regione Siciliana*, al fine di ridurre i rischi di violazioni della sicurezza conseguenti ad una condotta non idonea da parte del personale interno e/o dei consulenti esterni e/o di terze parti che concorrono a vario titolo alla gestione dei processi posti sotto la responsabilità della *Regione Siciliana*.Nell'ambito della presente politica sono trattate le seguenti tipologie di risorsa informatiche:

- **Informazioni contenute in documenti digitali e database informatici**, relativi ad esempio a:
  - Proprietà intellettuale;
  - Know-how;
  - Missione istituzionale;
  - Informazioni contabili/finanziarie;
  - Informazioni sui dipendenti;
  - Informazioni su clienti, fornitori e partner;
  - Documentazione del sistema di sicurezza;
  - Procedure operative o di supporto;
  - Piani di continuità.
- **Risorse software**: applicazioni, software di base, middleware, ambienti di sviluppo, programmi di utilità, facilities informatiche ecc.;
- **Risorse hardware**: apparecchiature informatiche (ad es. server, client ovvero PC fissi e portatili, monitor, sistemi di backup e restore), apparecchiature di comunicazione (ad es. router, switch, fax, segreterie telefoniche), supporti magnetici (ad es. nastri e dischi), altre apparecchiature tecniche (ad es. alimentazioni elettriche, unità di climatizzazione, mobili).

Le indicazioni formulate nel presente documento sono da intendersi come un insieme di misure minime la cui osservanza contribuisce a ridurre i rischi di violazioni della sicurezza informatica derivanti da errati comportamenti da parte del personale operante presso la*Regione Siciliana*.

1.2 Ambito di Applicabilità

Le raccomandazioni formulate in questa sedesono rivolte a tutti i dipendenti o collaboratori della *Regione Siciliana*, che forniscono le proprie prestazioni lavorative a qualsiasi titolo e sotto qualsiasi forma contrattuale.

Sono altresì tenuti al rispetto della politica, tutti i soggetti che accedono ai sistemi informatici della *Regione Siciliana*, nonché i visitatori e gli ospiti occasionali. In particolare, sono tenuti al rispetto della politica di sicurezza i fornitori di servizi informatici applicativi o di servizi di gestione/amministrazionedegli apparati/sistemi informatici.

Resta inoltre inteso che:

- Per le risorse informatiche messe a disposizione o date in uso alla *Regione Siciliana*da altri enti od organizzazioni pubbliche e private, valgono gli accordi e le condizioni contrattuali o i protocolli di intesastipulati fra le parti;
- Per l'utilizzo di documenti digitali, banche dati, programmi e materiali di proprietà di altri soggetti esterni alla *Regione Siciliana*, valgono le condizioni di tutela del diritto d'autore o del copyright, ove previsto;
- Le modalità di utilizzo delle risorse informatiche devono essere sempre conformi a quanto previsto dalle normative vigenti.

Tutte le funzioni organizzative della *Regione Siciliana*sono tenute all'osservanza della presente politica ed i responsabili di ciascuna funzione sono tenuti a farne rispettare le prescrizioni.

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 ProtectionRegulation (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.	--	Deliberazione del Garante Privacy numero 53 del 23 novembre 2006: Linee guida in materia di trattamento di dati personali di lavoratori
DR-4.	--	Deliberazione del Garante Privacy numero 13 del 1° marzo 2007: Linee guida del Garante per posta elettronica e internet
DR-5.	--	Provvedimento del Garante Privacy del 13 ottobre 2008: Smaltimento e cancellazione sicura dei dati
DR-6.	--	Provvedimento del Garante Privacy dell'8 aprile 2010: Videosorveglianza
DR-7.	--	Provvedimento del Garante Privacy: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – 27 novembre 2008 e successive modifiche e integrazioni
DR-8.	--	Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS)

Rif.	Codice	Titolo
DR-9.	--	D.lgs. 65/2018: Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" (Attuazione Direttiva (UE) NIS 2016/1148)
DR-10.	--	Legge 22 aprile 1941 n.633: Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" e successive modifiche e integrazioni, in particolare D.lgs. n.8 del 15 gennaio 2016: Disposizioni in materia di depenalizzazione
DR-11.	--	Legge 23 dicembre 1993 n. 547: Modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica
DR-12.	--	ISO 9001:2008: Sistemi di Gestione per la Qualità – Requisiti
DR-13.	--	ISO/IEC 73:2009: Risk management – Vocabulary – Guidelines for use in standards
DR-14.	--	UNI ISO 31000:2010: Gestione del rischio – Principi e linee guida
DR-15.	--	ISO/IEC 27001: Tecnologie Informatiche –Tecnicheper la Sicurezza –Sistemidi Gestione per la Sicurezza delle Informazioni – Requisiti
DR-16.	--	ISO/IEC 27002: Information Technology – Security Techniques –Codeof practice for information security management
DR-17.	--	ISO/IEC 27003: Information Technology – Security Techniques – Information security management system implementation guidance
DR-18.	--	ISO/IEC 27004: Information Technology – Security Techniques – Information security management – Measurement
DR-19.	--	ISO/IEC 27005: Information Technology – Security Techniques – Information security risk management
DR-20.	--	D.lgs. n. 82/2005: Codice dell'amministrazione digitale e successive modificazioni e integrazioni
DR-21.	--	Misure minime di sicurezza per le PA (AgID)
DR-22.	--	D.lgs. n.203 del 6 novembre 2007 (limitatamente agli aspetti correlati alla sicurezza informatica e cibernetica)
DR-23.	--	DPR n.63 del 16 aprile 2013 - Codice di comportamento dei dipendenti pubblici
DR-24.	--	Politica per la gestione delle utenze – Regione Siciliana
DR-25.	--	Politica per la gestione e la comunicazione di violazioni della privacy (data breach)– Regione Siciliana
DR-26.		Regole per il trattamento dei dati personali sulle piattaforme e sui sistemi informativi: Piattaforma PROXY SERVER - Regione Siciliana

Tabella 2 - Documenti di Riferimento

3 DEFINIZIONI E ACRONIMI

3.1 Definizioni

Vocabolo	Titolo

Tabella 3 - Definizioni

3.2 Acronimi

Codice	Titolo
AgID	Agenzia per l'Italia Digitale
Amministrazione	CONSIP
c.p.	Codice penale
CE	Contratto Esecutivo
Committente	CONSIP
CQ	Contratto Quadro
Fornitore	Vedi Raggruppamento
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 PRINCIPI GENERALI

In conformità a quanto disposto nel Codice di comportamento del personale dipendente delle pubbliche amministrazioni [DR-23] (nel seguito Codice), i rapporti e i comportamenti, a tutti i livelli gerarchici, sono improntati a principi di diligenza, lealtà, imparzialità e buona condotta. Tali principi si applicano anche alle norme interne ed alle raccomandazioni disposte dalla *Regione Siciliana*per la tutela e la sicurezza delle proprie risorse informatiche.

Il personale autorizzato deve utilizzare le risorse informatiche della *Regione Siciliana* per esclusive finalità lavorative, nella consapevolezza che queste costituiscono un bene da custodire e tutelare. In particolare, le informazioni, i documenti digitali, i dati e le conoscenze, sono acquisite, utilizzate e comunicate da parte del personale autorizzato in virtù delle mansioni affidate, esclusivamente per perseguire gli scopi istituzionali della *Regione Siciliana*.

L'autorizzazione all'uso delle risorse informatiche è pertanto:

- Strettamente personale e non cedibile;
- Subordinata alla durata temporale del rapporto di lavoro o di collaborazione con la *Regione Siciliana*;
- Strettamente funzionale all'espletamento degli incarichi affidati.

È vietata qualsiasi attività che possa produrre danni, diretti o indiretti, alle risorse informatiche e che risulti in contrasto con le regole contenute nel presente documento e più in generale con le altre normative emanate dalla *Regione Siciliana*o contrarie alla legislazione vigente.

4.1 Obblighi e Responsabilità dell'utente

Con il termine utente si definisce qualsiasi soggetto che, nell'espletamento delle proprie mansioni abbia la necessità di usufruire delle risorse informatiche messe a disposizione dalla *Regione Siciliana*. In tale ambito è pertanto vietato l'impiego di tali risorse per scopi personali o di terzi in quanto può determinare disservizi o minacce alla sicurezza dei dati; in particolare, è vietato:

- Impiegare le risorse per finalità diverse da quelle per le quali sono state progettate o utilizzare i sistemi informatici per compiere azioni illecite nei confronti di altri sistemi, sia interni che esterni, alla *Regione Siciliana*;
- Recare volontariamente danni alle risorse della *Regione Siciliana*, agli strumenti di supporto, ed in generale ai dispositivi informatici utilizzati dalla *Regione Siciliana*.

Ogni risorsa, concessa ai fini esclusivamente lavorativi, deve essere custodita con diligenza e mantenuta in buono stato dall'utente affidatario. È responsabilità dell'utente affidatario richiedere gli interventi manutentivi opportuni, segnalando tale necessità alla funzione organizzativa competente.

Tutte le dotazioni hardware e software fornite in dotazione sono di proprietà della *Regione Siciliana*; l'utente è consapevole ed accetta di restituire la totalità delle risorse informatiche utilizzate nel momento in cui cessiil rapporto con la *Regione Siciliana*, oppure nel caso di variazione di mansione o passaggio ad altro servizio o ad altra funzione organizzativa.

Il personale della *Regione Siciliana* che contravviene a tali disposizioni o alle norme d'uso di seguito riportate, sarà ritenuto responsabile, a seconda dei casi, disciplinarmente e giuridicamente.

Tutto il personale operante presso la *Regione Siciliana* deve esseresensibilizzato e reso consapevoledel fatto che taluni comportamentinon autorizzati, oltre che eticamente scorretti,possono costituire anche un illecito perseguibile nell'ambito dell'ordinamento giuridico italiano.

Nei paragrafi successivi sono brevemente descritti gli ambiti normativi che possono dare luogo a sanzioni disciplinari e/o illeciti amministrativi e/o imputazioni penali.

4.2 Violazioni della privacy

Ai sensi del Regolamento Europeo in materia di protezione dei dati personali, GDPR 2016/679 [DR-1], e al D.lgs. n. 101 del 2018 [DR-2], il trattamento illecitodi dati personali detenuti e gestiti dalla *Regione Siciliana* e/o la mancata osservanza delle misure di sicurezza previste per la loro protezione, possono essere sanzionabili. Pertanto, tutti i soggetti che a vario titolo svolgono trattamenti di dati personali sottoposti alla titolarità della *Regione Siciliana*, devono attenersi come minimo alle seguenti regole di carattere generale:

- Osservare scrupolosamente le disposizioni impartite dal Titolare[1] in materia di trattamento dei dati personali;
- Non trattare, comunicare o diffondere i dati personali per finalità o con modalità diverse da quelle strettamente riconducibili agli scopi della *Regione Siciliana*;
- Applicare e/o favorire l'applicazione delle misure di sicurezza informatica adottate per la loro protezione.

4.3 Violazioni del diritto d'autore

Per quanto riguarda la tutela del diritto d'autore e l'utilizzo del software e dei prodotti informatici, devono essere rispettate le politiche predisposte dalla *Regione Siciliana* atte ad assicurare un utilizzo delle risorse conforme alle disposizioni normative che tutelano il copyright i brevetti e la proprietà intellettuale [DR-10].

Pertanto, tutto il personale deve utilizzare il software installato sulla postazione lavorativa (personal computer o dispositivi mobili) o disponibile attraverso la rete interna, nel rispetto dei termini contrattualie/o delle licenze in concessione d'uso, osservandone attentamente le limitazioni relative, ad esempio, al numero di copie riproducibili, al numero di utenti fruitori ed alle scadenze temporali delle concessioni.

4.4 Violazioni riconducibili a crimini informatici

Costituisce un reato punibile penalmente il compimento di atti e comportamenti, configurabili come "crimini informatici", quali ad esempio:

- L'esercizio arbitrario delle proprie ragioni con violenza sulle cose (art. 392 c.p.);
- L'attentato ad impianti informatici di pubblica utilità (art. 420 c.p.);
- La falsificazione di documenti informatici (art. 491 bis c.p.);
- 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.);
- La diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies c.p.);
- La violazione di corrispondenza telematica (artt. 616 e 617 sexies c.p.);
- L'intercettazione di e-mail (art. 617 quater c.p.);
- La rivelazione del contenuto di documenti segreti (art. 621 c.p.);
- Il danneggiamento di sistemi informatici e telematici (art. 635 bis c.p.);
- La frode informatica (art. 640 ter c.p.) ovvero l'alterazione dell'integrità dei dati allo scopo di procurarsi un illecito profitto.

In caso di accertate violazioni delle norme sopra indicate si dovrà provvedere all'immediata inibizione delle credenziali di accesso personali riconducibili alla persona fisica in presunzione di reato, fermo restando ogni ulteriore provvedimento di carattere sanzionatorio[DR-11].

[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).

5 NORME PER L'UTILIZZODELLE RISORSE INFORMATICHE

Nei paragrafi successivi sono esposte le raccomandazioni ed i vincoli che regolamentano l'accesso e l'utilizzo del patrimonio informatico della *Regione Siciliana*.

L'utilizzo di dispositivi personali come notebook, tablet, smartphone, PDA (Personal Digital Assistance), dispositivi removibili (hard disk portatili, chiavette USB, DVD ecc..), pone una serie di minacce ai dati memorizzati e/o processati attraverso l'uso di tali dispositivi.

Tali minacce, dovute ad esempio alla perdita/furto del dispositivo mobile o la presenza di codice malevolo, possono causare l'accesso non autorizzato ai dati della *Regione Siciliana*.

Per tali motivi, non è autorizzato l'utilizzo di dispositivi personali da parte degli utenti della *Regione Siciliana* per lo svolgimento delle proprie attività lavorative.

Nei paragrafi successivi sono descritte le misure di sicurezza che devono essere attuate per l'accesso e l'utilizzo delle risorse informatiche della *Regione Siciliana*. Ulteriori misure di sicurezza su tematiche specifiche sono previste nell'ambito di apposita documentazione emessa dalla *Regione Siciliana.*

5.1 Accesso alle risorse informatiche

Gli utenti sono autorizzati ad accedere alle risorse informatiche della *Regione Siciliana*esclusivamente per lo svolgimento delle mansionilavorative ad essi affidate.

In questo ambito, ogni soggetto autorizzato è tenuto a adottaretutte le misure di sicurezza necessarie a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche di proprietà della *Regione Siciliana* e a segnalare al proprio responsabile, eventuali presunte violazioni alle suddette prescrizioni.

Gli strumenti adottati dalla *Regione Siciliana* per l'accesso alle risorse informatiche (es. codici di accesso, user-id) sono di uso strettamente personale e pertanto l'utente è tenuto a custodirli in modo appropriato, nel rispetto dei principi descritti al paragrafo 5.1.1del presente documento.

5.1.1 Gestione degli account

L'accesso alle risorse informatiche è riservato al personale autorizzato munito di credenziali di accesso(useraccount o più semplicemente utenza). L'account è strettamente personale e pertanto non ne è consentito l'utilizzo da parte di persone diverse dal titolare assegnatario, né questi può cederlo a terzi anche solo temporaneamente.

Il titolare assegnatario dell'utenza è direttamente responsabile di tutte le transazioni e le operazioni eseguite tramite il suo account.

Le credenziali di autenticazione di ciascun account sono compostecome minimo da due entità logiche: un identificativo utente (user-id) ed una password personale.

In particolare, l'identificativo utente:

- Deve essere assegnato da un amministratore incaricato ed autorizzato dalla *Regione Siciliana*;
- Deve osservare regole semantiche che consentano l'identificazione univoca dell'utente senza tuttavia rivelarne l'identità personale.

La password:

- Deve essere creata esclusivamente dall'utente assegnatariodell'account;
- Deve essere mantenuta riservata e non può essere comunicata ad alcuno;
- Deve osservare le regole definite nella specifica politica [DR-24] (es. lunghezza, composizione di caratteri e ciclo di vita).

La password iniziale di accesso attribuita ad una nuova utenza è assegnata dalle funzioni organizzative preposte e deve essere obbligatoriamente modificata dall'utente assegnatario al primo utilizzo.

5.2 Utilizzo delle apparecchiature informatiche e telematiche

Ogni utente è responsabile della corretta custodia dei dispositivi informatici e telematici ricevuti in dotazione così come delle informazioni in essi custodite.

Al fine di garantire un utilizzo diligente delle risorse informatiche, ogni soggetto autorizzato deve pertanto attenersi alle seguenti disposizioni minime:

- Utilizzarle unicamente per lo svolgimento delle attività lavorative, nell'ambito delle mansioni assegnate ed esclusivamente per scopi leciti;
- Qualora necessario, non cedere la postazione di lavoro (PC) ad altri soggetti senza prima aver chiuso tutte le sessioni e le istanze elaborative riconducibili al proprio account personale;
- Qualora disponibili, attivare le funzioni di oscuramento temporizzato del videocon sblocco tramite password, quando ci si allontana ,anche temporaneamente, dalla propria postazione di lavoro;
- Avere cura di spegnere il PCal termine dell'orario di lavoro a meno che non sia strettamente necessario mantenere attiva una sessione elaborativa.

Per assicurare il corretto funzionamento delle applicazioni e per evitare violazioni della sicurezza informatica (ad es. accessi abusivi, propagazione di virus informatici, trattamentiilleciti, ecc.) è inoltre opportuno:

- Non modificare, senza preventiva autorizzazione, le configurazioni impostate sulle apparecchiature informatiche e telematiche affidate in uso;
- Non installare ed eseguire alcun software se non preventivamente verificato dal proprio referente informatico, a meno che il software non sia inserito in una lista dei software di uso consentito;
- Non connettere allesuddette apparecchiature informatiche e telematiche, alcun tipo di perifericapersonalenon fornita dalla *Regione Siciliana* quali ad esempio dispositivi bluetooth, masterizzatori, smartphone o altri dispositivi mobili.

Gli utenti autorizzati all'utilizzo di PC portatili o altri dispositivi mobili di proprietà della *Regione Siciliana*devono inoltre assicurare:

- Una diligente applicazione delle procedure di manutenzione ordinaria (es. aggiornamenti software);
- La tutela delle informazioni custodite, adottando le misure di sicurezza messe a disposizione dal sistema e/o fornite dalla *Regione Siciliana*;
- L'esecuzione di copie di sicurezza (backup) settimanale del lavoro svolto nell'arco della settimana su un supporto che dovrà essere custodito separatamente dal computer ovvero su una cartella di un computer diverso, purché questa sia protetta da password personale che abiliti l'accesso esclusivo ai dati contenuti. Nel casodi backup effettuato tramite servizi incloudai documenti dovranno essere applicate le medesime misure di sicurezza previste per le informazioni originali. Le copie di backup potranno essere utilizzate esclusivamente per il fine per cui sono state effettuate: è vietato ogni altro utilizzo;
- In caso di constatazione di furto o smarrimento, l'utente assegnatario, oltre ad attenersi alle normali disposizioni previste per la perdita di beni della *Regione Siciliana*, deve darne immediata comunicazione alpersonale preposto alla gestione degli incidentiinformatici, segnalando la tipologia di informazioni custodite nel dispositivo, al fine di consentire l'eventuale attivazione delle procedure di gestione delle violazioni di sicurezza informatica (data breach) [DR-25].

I dispositivi di identificazione/autenticazione forte (smart card, token OTP, dispositivi biometrici ecc.), laddove previsti, sono affidati direttamente al singolo utente, che ne risponde a titolo penale, disciplinare e patrimoniale. Essi non devono mai essere ceduti, ancorché temporaneamente a terzi, ivi compresi collaboratori, colleghi o persone di stretta fiducia. In caso di furto o smarrimento di tali dispositivi, l'utente

assegnatario deve darne immediata comunicazione al personale preposto alla gestione degli incidenti informatici, al fine di attivare prontamente le procedure di blocco delle credenziali di accesso.

In caso di riutilizzo/dismissione dei personal computer, l'utente assegnatario prima della riconsegna, deve preventivamente assicurarsi che le informazioni eventualmente custodite vengano cancellate in modo da garantire la non recuperabilità delle stesse.

5.3 Utilizzo dei supporti di archiviazione rimovibili

Con il termine supporto di archiviazione rimovibile s'intende ogni dispositivo esterno alle unità elaborative, utilizzabile per la custodia ed il trasporto di dati in formato elettronico, quali ad esempio flash drive USB, CD ROM, hard disk esterni ecc.

Fatto salvo ulteriori restrizioni applicabili al trattamento di determinate tipologie di dati (es. dati classificati, categorie particolari di dati personali, ecc.) si raccomanda l'applicazione delle seguenti raccomandazioni:

- Non è consentito l'utilizzo di supporti rimovibili personali per l'archiviazione ed il trasporto di informazioni della *Regione Siciliana*;
- In caso di dismissione dei supporti di archiviazione rimovibile, l'utente deve assicurarsiprima dello smaltimento, che i dati in essi contenuti vengano cancellati in modo da garantirne la non recuperabilità;
- Nel caso di dismissione dei supporti CD ROM/DVD, questi dovranno essere resi fisicamente inutilizzabili.

5.4 Utilizzo delle risorse di rete e dei canali di comunicazione

L'utilizzo delle risorse di rete e dei canali di comunicazione messi a disposizione della *Regione Siciliana*quali ad esempio la intranet, la PEC, la posta elettronica, la navigazione Interneted i servizi di interoperabilità SPC, devono essere strettamente funzionaliallo svolgimento delle attività lavorative.

Nei paragrafi successivi sono dettagliate le raccomandazioni di utilizzo delle risorse di rete più comune in ambito *Regione Siciliana*.

5.4.1 Utilizzo della posta elettronica

La posta elettronica rappresenta uno dei canali preferenziali per la veicolazione di attacchi informatici e pertanto il suo utilizzo richiede l'osservanza di regole comportamentali volte a minimizzare i rischi di propagazione di virus informatici, messaggi di spamming,ramsonware ed altre tipologie di software malevolo.

Le raccomandazioni di seguito esposte riguardano l'utilizzo delle caselle di posta elettronica appartenenti al dominio *@regione.sicilia.it*.

La casella di posta assegnata al personale interno (dipendenti/consulenti), costituisce uno strumento di lavoro messo a disposizione dalla *Regione Siciliana* per favorire le comunicazioni necessarie allo svolgimento delle attività lavorative. Non è pertanto consentito:

- Inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione politica;
- Effettuare ogni genere di comunicazione di caratterefinanziario svolta a titolo personale, come ad esempio operazioni di remote banking, trading online, acquisti o prenotazioni online;
- Utilizzare l'indirizzo di posta elettronica della *Regione Siciliana*come account di iscrizione o come canale di comunicazione per la partecipazione a dibattiti, forum, mailing-list o social network, salvo diversa ed esplicita autorizzazione da parte del proprio responsabile;
- Utilizzare liste di distribuzione per inoltrare messaggi, comunicazioni o allegati non attinenti all'ambito lavorativo (spamming);

- Inviare messaggi a contenuto commerciale, pubblicitario e comunque non attinente alle attività lavorative;
- Aprire file allegati, o link a indirizzi web inseriti nel testo dei messaggi, provenienti da mittenti sconosciuti o che presentino caratteristiche sospette.

5.4.2 Utilizzo di Internet e del Web

La *Regione Siciliana* fornisce, limitatamente agli uffici/funzioni che ne hanno necessità, l'accesso alla rete Internet ed ai siti Webdalle postazioni di lavoro di propria competenza. L'utilizzo è consentito esclusivamente per scopi leciti e legati alle attività lavorative ed è subordinato al rispetto delle seguenti raccomandazioni:

- È vietata la navigazione verso siti Web che violino il Codice [DR-23] o che comunque siano in contrasto con le normative vigenti o con normative specifiche emanate dalla *Regione Sicilia;*
- Èassolutamente vietato l'accesso a siti Web di giochi online, compreso quelli a scopo puramente ludico;
- Non è consentita la partecipazione, anche anonima o attraverso registrazioni temporanee, a forum, chat line, bacheche elettroniche e social networkche non siano pertinenti con gli scopi lavorativi;
- Èvietato l'utilizzo online o il download di qualsiasi tipologia di software, anche se utile allo svolgimento dell'attività lavorativa, se non preventivamente autorizzato dalla funzione preposta alla gestione dell'infrastruttura IT;
- Èvietato il download di fileche presentino contenuti di natura oscena, blasfema, diffamatoria, oltraggiosa o discriminatoria per sesso, lingua, religione, etnia, opinione o idea politica;
- Èvietato il download o lo scambio peer-to-peer di materiale audiovisivo, fotografico, software ed in genere di ogni altra tipologia di materiale digitale che possa sottintendere presunte o palesi violazioni del copyright in ambito nazionale ed internazionale.
- È vietato collegare alla rete della *Regione Sicilia*, modem o altri dispositivi che consentano un accesso non controllato alla risorse informatiche della *Regione Siciliana*.

La navigazione Web effettuata in conformità al primo punto del precedente elenco è subordinata altresì al rispetto di specifiche regole emanate dalla *Regione Siciliana* [DR-26].

5.4.3 Utilizzo delle reti interne (Intranet)

Le reti interne della *Regione Siciliana* costituiscono un'area riservata, necessaria alla condivisione di servizi/informazioni che supportano l'espletamento degli scopi istituzionali della *Regione Siciliana*. Per tali motivi, le reti interne si configurano come un asset infrastrutturale critico per il corretto svolgimento dei processi e delle attività lavorative e sono sottoposte alle seguenti raccomandazioni d'uso:

- L'accesso alle reti interne, da parte dei soggetti autorizzati, è subordinato all'identificazione e all'autenticazione delle credenziali di accesso personali;
- La creazione di cartelle condivise per la custodia di file accessibili a gruppi di utenti autorizzati deve essere approvata dal proprio Dirigente Responsabile;
- Non è consentita la condivisione di informazioni non pertinenti allo svolgimento delle attività lavorative.

Nel caso in cui, per l'esecuzione delle attività lavorative, sia necessario l'accesso da remoto alle reti interne, devono essere applicate le seguenti raccomandazioni aggiuntive:

- L'accesso da remoto deve avvenire esclusivamente attraverso canali di comunicazione sicuri (es. VPN);
- Non è consentito l'accesso da remoto attraverso dispositivi personali di uso domestico, se nonin casi di estrema necessità ed urgenza e comunque esplicitamente autorizzati da parte del proprio referente informatico;
- Evitare per quanto possibile l'accesso in remoto da dispositivi situati all'aperto o in luoghi pubblici affollati.