

	<b>Politica per la sicurezza delle informazioni</b>	Versione 1.0
POL_POL_01_PoliticaGenerale_v1.0.docx	Classificazione: Pubblico	

# POL01

## Politica per la sicurezza delle informazioni

Redatto	Verificato	Approvato
Data: 17/10/2016	Data: 5/12/2016	Data:
Firma:	Firma:	Firma:
Fabio Bucciarelli	Fabio Bucciarelli	Stefania Papili
Classificazione del documento:	Pubblico	

	<b>Politica per la sicurezza delle informazioni</b>	Versione 1.0
POL_POL_01_PoliticaGenerale_v1.0.docx	Classificazione: Pubblico	

## INDICE

Introduzione	3
Storia del documento	3
Documenti allegati	3
Glossario	3
Scopo ed obiettivi	4
Campo di applicazione	4
Contestualizzazione	4
Classificazione del documento	8
Ruoli e responsabilità	8
Compliance	8

	<b>Politica per la sicurezza delle informazioni</b>	Versione 1.0
POL_POL_01_PoliticaGenerale_v1.0.docx	Classificazione: Pubblico	

## 1 Scopo ed obiettivi

La Giunta Regionale e l'Assemblea Legislativa della Regione Emilia-Romagna (di seguito Ente) considerano le informazioni gestite nell'ambito della sua attività istituzionale parte integrante del proprio patrimonio istituzionale.

La tutela del patrimonio delle informazioni riveste importanza strategica per l'Ente, oltre che essere soggetta a precisi vincoli normativi.

La sicurezza delle informazioni è definita come la salvaguardia di riservatezza, integrità e disponibilità delle stesse.

In particolare:

1. tutelare la *riservatezza* significa assicurare che le informazioni siano accessibili solo a coloro che sono autorizzati ad avervi accesso;
2. tutelare l'*integrità* significa salvaguardare l'accuratezza e la completezza delle informazioni e del loro trattamento;
3. tutelare la *disponibilità* significa assicurare che gli utenti autorizzati abbiano accesso, quando richiesto, alle informazioni e agli strumenti ad esse associati.

Per questi motivi la Giunta Regionale adotta un Sistema di Gestione per la Sicurezza Informatica (SGSI) secondo lo standard internazionale ISO/IEC 27001:2013.

## 2 Campo di applicazione

La politica di sicurezza delle informazioni si applica all'Ente nell'ambito di tutte le sue funzioni istituzionali. In particolare si applica alla gestione della sicurezza dei dati e delle informazioni nelle attività svolte dal Servizio ICT Regionale della Giunta e dal Servizio Funzionamento e Gestione dell'Assemblea Legislativa.

La politica si applica a tutte le informazioni trattate nell'ambito sopra definito, qualsiasi natura e forma esse abbiano o prendano, e a tutti i sistemi di gestione e supporti di memorizzazione utilizzati per il loro trattamento e conservazione.

I destinatari della politica sono tutti i collaboratori dell'Ente, dipendenti o non dipendenti. Sono tenuti al rispetto della politica tutti i soggetti che a vario titolo fruiscono dei servizi informativi dell'Ente, nonché i visitatori e gli ospiti. In particolare, sono tenuti al rispetto della politica di sicurezza, i fornitori di servizi informatici che operano direttamente sui sistemi di gestione delle informazioni.

	<b>Politica per la sicurezza delle informazioni</b>	Versione 1.0
POL_POL_01_PoliticaGenerale_v1.0.docx		Classificazione: Pubblico

### 3 Contestualizzazione

L'applicazione ed il mantenimento della sicurezza si attuano attraverso misure tecniche e misure organizzative che devono essere recepite dai processi di lavoro per diventarne parte integrante.

Prerequisito della politica di sicurezza delle informazioni è il rispetto delle misure di sicurezza minime ed idonee definite dalla normativa applicabile all'ambito della Giunta Regionale e dell'Assemblea Legislativa

La costruzione di un adeguato processo di gestione della sicurezza comprende le seguenti fasi distinte:

1. *pianificazione della sicurezza*: definizione degli obiettivi di sicurezza, analisi dei rischi, individuazione delle misure di sicurezza;
2. *implementazione delle misure di sicurezza*: messa in opera delle misure di sicurezza individuate;
3. *controlli*: verifica dell'efficienza e della corretta applicazione delle misure di sicurezza adottate;
4. *revisioni*: attuazione di correzioni ed adeguamenti al sistema di protezione delle informazioni sulla base dei risultati ottenuti dai controlli applicati e dagli aggiornamenti normativi e tecnologici.

La scelta delle misure da rendere esecutive è quindi effettuata a seguito di un'analisi costi/benefici (analisi dei rischi) e tale analisi è costantemente ripetuta nel tempo alla luce dei progressi tecnologici, dei mutamenti normativi e del riscontro ottenuto dai controlli sulle misure già adottate.

#### Sensibilizzazione

La sicurezza di un sistema è costituita da tecnologie, procedure e comportamenti di tutti gli utenti del sistema stesso. Ciò rende fondamentale la sensibilizzazione di tutti coloro che effettuano trattamenti di dati personali e di informazioni ritenute riservate circa i rischi incombenti sui dati e circa il corretto utilizzo dei relativi strumenti di protezione disponibili.

I sistemi e le reti d'informazione sono sottoposti a rischi interni ed esterni, è quindi necessario porre in essere azioni di sensibilizzazione finalizzate a creare nei destinatari della presente politica la consapevolezza che, a causa dell'interconnessione e dell'interdipendenza tra sistemi, le falle in materia di sicurezza su un componente del sistema possono propagare i loro effetti fino ad incidere gravemente sull'integrità dei sistemi, delle reti, delle banche dati, degli archivi e arrecare danni ad altri.

Comportamenti non partecipi, disinformati o indifferenti, possono ostacolare gravemente la tutela del patrimonio informativo e ledere il rapporto di fiducia che deve necessariamente intercorrere tra

	<b>Politica per la sicurezza delle informazioni</b>	Versione 1.0
POL_POL_01_PoliticaGenerale_v1.0.docx		Classificazione: Pubblico

l'Amministrazione regionale e la società civile.

### **Uso delle strumentazioni informatiche**

Le strumentazioni informatiche che l'Ente mette a disposizione devono essere utilizzate in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.

Con specifico riferimento agli strumenti informatici e telematici, alla posta elettronica e a Internet, i destinatari della presente politica sono tenuti in particolare a:

1. utilizzare tali beni per motivi non attinenti all'attività lavorativa soltanto in casi di urgenza e comunque non in modo ripetuto o per periodi di tempo prolungati;
2. utilizzare la posta elettronica e Internet nel rispetto del principio di riservatezza, per le specifiche finalità della propria attività istituzionale e rispettando le esigenze di funzionalità della rete e quelle di semplificazione dei processi lavorativi.

### **Segnalazione delle violazioni**

Le violazioni di sicurezza interna o gli eventi che possono portare a credere che vi sia stata un'elusione delle misure di sicurezza previste, devono essere tempestivamente segnalate secondo le modalità e le regole tecniche definite da uno o più documenti specifici.

### **Controlli di sicurezza**

L'Ente effettua i controlli ritenuti opportuni per la verifica della corretta applicazione e dell'efficienza delle misure di sicurezza adottate per la protezione dei dati personali.

Tali controlli sono effettuati esclusivamente da personale debitamente autorizzato.

### **Controllo degli accessi fisici**

L'accesso e la permanenza all'interno delle sedi dell'Ente sono consentiti esclusivamente alle persone autorizzate.

Le aree dove sono situati i sistemi e le apparecchiature di elaborazione dei dati sono dotate di un ulteriore meccanismo di controllo accessi basato su badge e di sistemi di videosorveglianza.

### **Controllo degli accessi logici**

L'accesso ai dati e alle informazioni trattati con strumentazioni informatiche avviene esclusivamente previa autenticazione, ossia tramite una procedura che verifica anche indirettamente l'identità di chi vi accede.

	<b>Politica per la sicurezza delle informazioni</b>	Versione 1.0
POL_POL_01_PoliticaGenerale_v1.0.docx		Classificazione: Pubblico

Ogni utente deve custodire le proprie credenziali di accesso ai sistemi, adottando le necessarie cautele per assicurare la segretezza della componente riservata e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo.

Ogni utente deve poter accedere solo all'insieme minimo di risorse necessarie allo svolgimento del proprio lavoro.

### **Gestione degli asset**

Deve esistere un catalogo costantemente aggiornato degli asset rilevanti ai fini della gestione della sicurezza delle informazioni e per ciascuno deve essere individuato un responsabile.

### **Risposta agli incidenti di sicurezza**

Gli utenti del sistema informativo dell'Ente devono operare tempestivamente e in uno spirito di collaborazione per prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza nel minor tempo possibile anche al fine di ridurre gli impatti conseguenti alla rapidità della diffusione conseguente all'interconnessione dei sistemi e delle reti d'informazione.

## **4 Ruoli e responsabilità**

Con specifico provvedimento (DGR. n. 2416/2008 per la Giunta, DUP n. 29/2012) sono state disciplinate le responsabilità relative agli obblighi e agli adempimenti in materia di protezione dei dati personali, ripartendo compiti e funzioni tra i soggetti competenti tenuto conto della specifica organizzazione dell'Amministrazione. Tale articolazione di competenze è applicabile, in quanto compatibile, anche per tutte le attività che non contemplano il trattamento di dati personali.

In ragione della complessità organizzativa dell'Ente e della rilevanza attribuita alla sicurezza delle informazioni, la Giunta Regionale e l'Assemblea Legislativa hanno inoltre designato, ciascuno per il proprio ambito, il Responsabile della sicurezza, quale specifica figura con la responsabilità di operare per la sensibilizzazione, il coordinamento, la vigilanza e l'implementazione delle misure di sicurezza individuate. In particolare, i Responsabili hanno il compito di curare, ciascuno per il proprio ambito, la redazione del Documento programmatico sulla sicurezza, di elaborare disposizioni in materia di sicurezza e di effettuare audit sulle strutture dell'Ente, operando in sinergia con le figure apicali dirigenti, al fine di verificare il rispetto delle misure di sicurezza stabilite.

Coloro che gestiscono, sviluppano, progettano e forniscono prodotti e servizi nell'ambito dei sistemi informativi, devono agire in modo da garantire la sicurezza dei sistemi e delle reti, tutelare la riservatezza dei dati personali e diffondere informazioni utili per assicurare l'adozione di idonee pratiche di sicurezza.

Tutti gli utenti devono adoperarsi per elaborare e adottare pratiche esemplari e incoraggiare comportamenti che tengano conto degli imperativi di sicurezza e di tutela dei diritti altrui.

	<b>Politica per la sicurezza delle informazioni</b>	Versione 1.0
POL_POL_01_PoliticaGenerale_v1.0.docx	Classificazione: Pubblico	

La violazione delle policy discendenti dai principi definiti nella presente politica, ferme restando eventuali responsabilità penali, civili o amministrativo-contabili, è rilevante sotto il profilo disciplinare e di responsabilità dirigenziale.

## **5 Disposizioni finali**

Per la concreta attuazione dei principi e delle finalità indicate nel presente documento, verranno adottati, a cura dei Responsabili per la sicurezza della Giunta e dell'Assemblea Legislativa, uno o più disciplinari tecnici contenenti norme di dettaglio da portare a conoscenza dei destinatari con le modalità più opportune.