POLITICHE DI SICUREZZA

1 INTRODUZIONE
1.1 PREMESSA
1.2 PERIMETRO ORGANIZZATIVO

2 POLICY
2.1 PRINCIPI GENERALI
2.2 IDENTIFICAZIONE, CLASSIFICAZIONE E GESTIONE DELLE RISORSE
2.3 GESTIONE SICURA DEGLI ACCESSI LOGICI
2.4 NORME COMPORTAMENTALI PER LA GESTIONE SICURA DELLE RISORSE
2.5 PERSONALE E SICUREZZA
2.6 GESTIONE DEGLI EVENTI ANOMALI E DEGLI INCIDENTI
2.7 GESTIONE DELLA SICUREZZA FISICA
2.8 ASPETTI CONTRATTUALI CONNESSI ALLA SICUREZZA DELLE INFORMAZIONI
2.9 GESTIONE DELLA BUSINESS CONTINUITY
2.10 MONITORAGGIO, TRACCIAMENTO E VERIFICHE TECNICHE
2.11 CICLO DI VITA DEI SISTEMI E DEI SERVIZI
2.12 RISPETTO DELLA NORMATIVA

3 DEFINIZIONE DEI RUOLI E DELLE RESPONSABILITÀ

UNIONE DI COMUNI MONTANA AMIATA GROSSETANA	MANUALE GESTIONE PROTOCOLLO **ALLEGATO 3** **POLITICHE DI SICUREZZA**	

1 INTRODUZIONE

1.1 PREMESSA

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni che l'Unione di Comuni Montana Amiata Grossetana ha fatto propri al fine di realizzare e mantenere un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.
Tali principi sono concretizzati nelle Policy per la sicurezza delle informazioni, la quale rispecchia le reali esigenze derivanti dalle attività svolte dall'Unione.
La sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e degli elementi del sistema informativo responsabile della loro gestione.
In particolare, perseguire la sicurezza delle informazioni significa definire, conseguire e mantenere le seguenti proprietà delle stesse:

- **riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/oai processi debitamente autorizzati;
- **integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- **disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
- **autenticità**: garantire la provenienza dell'informazione;
- **non ripudio**: assicurare che l'informazione sia protetta da falsa negazione diricezione, trasmissione, creazione, trasporto e consegna.

La mancanza di adeguati livelli di sicurezza, in termini di riservatezza, disponibilità,integrità, autenticità e non ripudio, può comportare, nell'ambito di una qualsiasi attività del Unione, il danneggiamento dell'immagine del Unione stessa, la mancata soddisfazione dei soggetti utenti,, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria. .

Il presente documento, nel rispetto delle norme vigenti:

- sottolinea l'importanza di garantire la sicurezza delle informazioni e degli strumenti atti al trattamento delle stesse;
- è coerente con la volontà espressa dall'Unione di garantire la protezione del patrimonio informativo;
- ha come oggetto aspetti fisici, logici ed organizzativi del Sistema di Gestione della Sicurezza delle Informazioni.

1.2 PERIMETRO ORGANIZZATIVO

La presente policy si applica a tutto il personale dipendente del l'Unione e a tutti i soggetti che collaborano con l'Unione nell'ambito della gestione del sistema informativo.
La policy si applica inoltre a tutti i processi più in generale a tutte le risorse coinvolte nella gestione delle informazioni trattate dall'Unione.

2 POLICY

2.1 PRINCIPI GENERALI

I principi generali cui l'Unione si ispira nella gestione della sicurezza delle informazioni sono articolati nelle seguenti aree:

- Identificazione, classificazione e gestione delle risorse
- Gestione sicura degli accessi logici

- Norme comportamentali per la gestione sicura delle risorse comunali
- Personale e Sicurezza
- Gestione degli eventi anomali e degli incidenti
- Gestione della sicurezza fisica
- Aspetti contrattuali connessi alla sicurezza delle informazioni
- Gestione della continuità operativa
- Monitoraggio, tracciamento e verifiche tecniche
- Ciclo di vita dei sistemi e dei servizi
- Rispetto della normativa

Di seguito, si riporta, per ciascuna tematica, l'obiettivo e le linee guida definite dall'Unione

2.2 IDENTIFICAZIONE, CLASSIFICAZIONE E GESTIONE DELLE RISORSE

Obiettivo: *garantire la piena conoscenza delle informazioni gestite nell'Unione e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.*

- Deve esistere ed essere mantenuto aggiornato, nel corso del tempo un inventario i beni materiali ed immateriali da tutelare (informazioni, hardware, software, documentazioni cartacee e supporti di memorizzazione);
- Ogni risorsa (bene materiale/immateriale) deve essere direttamente associabile ad un responsabile.
- Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.

2.3 GESTIONE SICURA DEGLI ACCESSI LOGICI

Obiettivo: *garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti che non hanno i necessari diritti.*

- L'accesso alle informazioni da parte di ogni utente deve essere limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti.
- L'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinata al superamento di una procedura di identificazione ed autenticazione degli stessi.
- Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui e devono essere periodicamente sottoposte a revisione.
- E' necessario definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso.
- I sistemi che costituiscono l'infrastruttura ICT devono essere opportunamente protetti e segretati, in modo da minimizzare la possibilità degli accessi non autorizzati.

2.4 NORME COMPORTAMENTALI PER LA GESTIONE SICURA DELLE RISORSE INFORMATICHE

Obiettivo: *garantire che i dipendenti e i collaboratori dell'Unione adottino modelli di comportamento volti a garantire adeguati livelli di sicurezza delle informazioni.*

- Gli ambienti di lavoro e le risorse dell'Amministrazione devono essere utilizzati in modo congruo con le finalità per le quali sono state rese disponibili e garantendo la sicurezza delle informazioni trattate.
- Devono essere definite delle procedure per la gestione ed utilizzo delle informazioni sia su supporto digitale che su supporto cartaceo.
- I sistemi informatici dell'Amministrazione devono essere impiegati da dipendenti e dai collaboratori secondo procedure formalmente definite.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare ai principali obblighi normativi del Codice in materia di tutela dei dati personali (D.Lgs 196/2003) ed dal quanto disposto dal Codice dell'Amministrazione digitale (D.Lgs. 82/2005) e provvedimenti collegati.

2.5 PERSONALE E SICUREZZA

Obiettivo: *garantire che il personale che opera per conto dell'Unione (dipendenti e collaboratori), abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni.*

- I dipendenti dell'Unione che operano nel sistema informativo devono ricevere un'adeguata formazione inerente le tematiche di sicurezza dei dati.

2.6 GESTIONE DEGLI EVENTI ANOMALI E DEGLI INCIDENTI

Obiettivo: *garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza dell'Amministrazione siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul sistema.*

- Tutti i dipendenti e i collaboratori sono tenuti a rilevare e notificare, a chi di competenza e secondo adeguate procedure, eventuali problematiche legate alla sicurezza delle informazioni.
- Gli incidenti che possono avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e non, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure.
- Deve essere realizzato un sistema di registrazione e classificazione degli incidenti e degli eventi anomali per effettuare analisi volte al miglioramento dei livelli di sicurezza coerentemente con le reali problematiche riscontrate.

2.7 GESTIONE DELLA SICUREZZA FISICA

Obiettivo: *prevenire l'accesso non autorizzato alle sedi ed ai singoli locali li e garantire adeguati livelli di sicurezza alle aree e alle attrezzature mediante i quali vengono gestite le informazioni.*

- Deve essere garantita la gestione della sicurezza delle aree e dei locali tramite: l'individuazione delle aree e la classificazione dei locali in base alla criticità delle informazioni elaborate; e la definizione dei livelli adeguati di protezione.
- Deve essere garantita la sicurezza delle apparecchiature tramite: la definizione di un'adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni; la messa a disposizione delle risorse necessarie al loro funzionamento; la predisposizione di un adeguato livello di manutenzione.

2.8 ASPETTI CONTRATTUALI CONNESSI ALLA SICUREZZA DELLE INFORMAZIONI

Obiettivo: *assicurare la conformità con i requisiti normativi e con i principi legati alla sicurezza delle informazioni nei contratti con i fornitori.*

- Gli accordi con i fornitori che accedono alle informazioni e/o agli strumenti che le elaborano, devono essere basati su contratti formali contenenti opportuni requisiti di sicurezza.
- Gli accordi con i fornitori ove necessario, devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare alle principali richieste provenienti dal Codice in materia di tutela dei dati personali (D.Lgs 196/2003) ed a quanto disposto dal Codice dell'Amministrazione digitale (D.Lgs. 82/2005) e provvedimenti collegati.

.

2.9 GESTIONE DELLA CONTINUITÀ OPERATIVA

Obiettivo: *garantire la continuità dell'attività dell'Amministrazione e l'eventuale ripristino tempestivo dei servizi erogati colpiti da eventi anomali di una certa gravità, riducendo le conseguenze sia all'interno che all'esterno del contesto aziendale.*

Deve essere predisposto un piano di continuità che permetta all'Amministrazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto garantendo il ripristino dei servizi critici in tempi e con modalità che

consentano la riduzione delle conseguenze negative sul funzionamento e sull'erogazione dei servizi da parte dell'Amministrazione..
Deve essere assicurato il mantenimento e l'aggiornamento del piano e delle procedure di cui al punto precedente al fine di garantire l'efficacia del sistema nel tempo a fronte di eventuali cambiamenti organizzativi/tecnologici.

2.10 MONITORAGGIO, TRACCIAMENTO E VERIFICHE TECNICHE

Obiettivo: *garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di assicurare la sicurezza e la disponibilità dei servizi e delle relative informazioni.*

- I sistemi informativi devono essere periodicamente controllati in modo da valutare il corretto funzionamento dei sistemi di sicurezza, hardware e software, implementati, nonché l'eventuale presenza di vulnerabilità non riscontrate o conosciute in passato.
- Sulla base dei I risultati di tutte le attività di monitoraggio, tracciamento e verifica devono essere effettuate periodiche attività di analisi, volte all'identificazione delle aree critiche e delle opportune azioni correttive e migliorative.

2.11 CICLO DI VITA DEI SISTEMI E DEI SERVIZI

Obiettivo: *assicurare che gli aspetti di sicurezza siano inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.*

- Nella fase di progettazione e sviluppo devono essere opportunamente considerati gli aspetti di sicurezza.
- Nella fase di esercizio devono essere opportunamente considerati gli aspetti di sicurezza.
- Nella gestione dei servizi devono essere opportunamente considerati gli aspetti di sicurezza.

2.12 RISPETTO DELLA NORMATIVA

Obiettivo: *garantire il rispetto delle disposizioni di legge, di statuti, regolamenti e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni reputazionali.*

- Tutti i requisiti normativi e contrattuali in materia di sicurezza del sistema informativo e aventi impatto sul Sistema di Gestione della Sicurezza delle Informazioni devono essere identificati ed analizzati, al fine di valutarne gli impatti sull'organizzazione e sui sistemi informativi.
- I responsabili delle diversi settori devono assicurarsi, ciascuno nell'ambito di propria competenza, che tutte le politiche, le procedure, gli standard e in generale tutta ladocumentazione relativa alla sicurezza delle informazioni siano applicati e rispettati.

3 DEFINIZIONE DEI RUOLI E DELLE RESPONSABILITÀ

L'Unione, in coerenza con la normativa vigente, e sulla base della propria organizzazione individuerà la, struttura responsabile della gestione della sicurezza delle informazioni.
La struttura responsabile della gestione della sicurezza delle informazioni, per svolgere le proprie attività dovrà coordinarsi con il responsabile del sistema informativo e le strutture responsabili previste dal Codice dell'Amministrazione Digitale D.Lgs. 82/2005 e provvedimenti collegati quali il responsabile della gestione documentale e il responsabile della conservazione, nonché con il responsabile del trattamento dei dati personali previsto dal D.Lgs. 196/2003.
Nel caso che l'Unione non individui una specifica struttura responsabile della gestione della sicurezza delle informazioni compiti e funzioni relativi della gestione della sicurezza delle informazioni restano in capo al Responsabile del sistema informativo.