


# POLITICA PER LA SICUREZZA DELLE INFORMAZIONI



## OLOMEDIA s.r.l.

 Via Simone Cuccia 46, 90144 Palermo ( PA )

 Tel. (+39) 091 324014 / Fax. (+39) 06 92912979

 P.Iva, C.F. e CCIAA Palermo n° 05715380829 REA di PA 272172 / Capitale Sociale € 10.0000,00

 [www.olomedia.it](http://www.olomedia.it) 



## Sommario

|          |  |          |
|----------|--|----------|
| <b>1</b> | <b>Scopo e campo di applicazione</b>                           | <b>2</b> |
| <b>2</b> | <b>Documenti e norme di riferimento</b>                        | <b>2</b> |
| <b>3</b> | <b>Terminologia di base della sicurezza delle informazioni</b> | <b>2</b> |
| <b>4</b> | <b>Gestire la sicurezza delle informazioni</b>                 | <b>3</b> |
|          | 4.1 Obiettivi e misurazione                                    | 3        |
|          | 4.2 Requisiti della sicurezza delle informazioni               | 3        |
|          | 4.3 Controlli della sicurezza delle informazioni               | 3        |
|          | 4.4 Responsabilità   | 3        |
|          | 4.5 Comunicazione della politica                               | 4        |
| <b>5</b> | <b>Supporto nell'implementazione del GSA</b>                   | <b>4</b> |
| <b>6</b> | <b>Validità e responsabilità della politica</b>                | <b>4</b> |

| Rev. | Data       | Causale         | Resp. GSA        | Direzione      |
|------|------------|-----------------|------------------|----------------|
| 01   | 18/02/2019 | Prima Emissione | Daniele Mondello | Marcello Vetro |

## 1 Scopo e campo di applicazione

Scopo di questa politica è definire lo scopo, la direzione, i principi e le regole di base per la gestione della sicurezza delle informazioni. Questa Politica viene applicata all'intero **Sistema di Gestione Aziendale (GSA)**, armonizzazione del **Sistema di Gestione della Qualità** e del **Sistema di Gestione della Sicurezza delle Informazioni**, e si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.. I destinatari di questo documento sono tutti dipendenti di Olomedia, i clienti, i fornitori, nonché le parti esterne pertinenti.

## 2 Documenti e norme di riferimento

- La Norma ISO/IEC 27001, punto 5.2 e 5.3
- La norma ISO/IEC 27017 punto 5.1..1
- La norma ISO IEC 27018 punto 5.1..1
- Il campo di Applicazione del GSA
- La Valutazione del Rischio e la Metodologia per il Trattamento del Rischio
- La Dichiarazione di Applicabilità
- L'Elenco degli Obblighi Legali, Normativi e Contrattuali
- La Procedura per la Gestione degli Incidenti

## 3 Terminologia di base della sicurezza delle informazioni

**Riservatezza:** disponibilità delle informazioni solo a persone o sistemi autorizzati.

**Integrità:** modifica delle informazioni consentito solo a persone o sistemi autorizzati.

**Disponibilità:** accesso alle informazioni quando necessario solo alle persone autorizzate.

**Sicurezza delle Informazioni:** riservatezza, integrità e disponibilità delle informazioni.

**Sistema di Gestione Aziendale (GSA):** parte dei processi generali di gestione che si occupa della pianificazione, dell'implementazione, del mantenimento, del riesame e del miglioramento della sicurezza delle informazioni.

## 4 Gestire la sicurezza delle informazioni

### 4.1 Obiettivi e misurazione

Gli obiettivi generali per il **GSA** ed in particolare nella gestione della sicurezza delle informazioni sono i seguenti:

- ridurre i danni causati dai potenziali incidenti del 20% ogni anno;
- aumentare la consapevolezza delle risorse promuovendo la loro partecipazione almeno ad un corso all'anno
- eseguire almeno un assessment annuo sulla sicurezza;

Gli obiettivi sono in linea con gli obiettivi aziendali, la strategia e i piani aziendali dell'organizzazione. La strategia prevede: un maggiore coinvolgimento attivo nel processo decisionale strategico, ad ogni riunione aziendale porre attenzione sulle implicazioni della cybersecurity tra le funzioni aziendali, promuovere i cambiamenti nel comportamento degli utenti, favorire Insourcing contro outsourcing e promuovere la propensione naturale dell'azienda a migliorare la reputazione dell'azienda contro profitti. **RGSA** è responsabile del riesame di questi obiettivi generali del **GSA** e della definizione di nuovi obiettivi. Gli obiettivi per i singoli controlli di sicurezza o gruppi di controlli sono proposti dal **RGSA** e approvati da **DIR** nella **Dichiarazione di Applicabilità**. Tutti gli obiettivi devono essere ri-esaminati con frequenza almeno annuale. La **DIR** misura l'adempimento di tutti gli obiettivi. **RGSA** è responsabile della definizione dei metodi per misurare il raggiungimento degli obiettivi - le misurazioni sono eseguite almeno una volta all'anno e **RGSA** analizza e valuta i risultati della misurazione e li segnala alla Direzione come input per il riesame della **DIR**. **RGSA** è responsabile di registrare i dati sui metodi di misurazione, periodicità e i risultati nel **Rapporto di Misurazione**.

## 4.2 Requisiti della sicurezza delle informazioni

Questa politica e l'intero **GSA** devono essere conformi ai requisiti legali e normativi rilevanti per l'organizzazione nel campo della sicurezza delle informazioni, nonché agli obblighi contrattuali. Un elenco dettagliato di tutti i requisiti contrattuali e legali è riportato nell' **Elenco degli Obblighi Legali, Regolamentari e Contrattuali**.

## 4.3 Controlli della sicurezza delle informazioni

Il processo di selezione dei controlli (protezioni) è definito nella **Metodologia per la Valutazione del Rischio e per il Trattamento del Rischio**. I controlli selezionati e il loro stato di implementazione sono elencati nella **Dichiarazione di Applicabilità**. L'organizzazione utilizza per i suoi processi servizi di cloud computing di terze parti; i requisiti generali di sicurezza delle informazioni sono specificati dalla **Politica per la sicurezza in cloud e Politica per la privacy in cloud**.

## 4.4 Responsabilità

Le responsabilità relative al **GSA** sono le seguenti:

- La **DIR** è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato
- La **DIR** deve riesaminare il **GSA** almeno una volta all'anno o ogni volta che si verifici un cambiamento significativo, e preparare il rapporto riassuntivo della riunione. Scopo del riesame della **DIR** è stabilire idoneità, adeguatezza ed efficacia del **GSA**.
- **RGSA** è responsabile di garantire che il **GSA** sia implementato e mantenuto conforme a questa politica e di garantire che tutte le risorse necessarie siano disponibili
- **RGSA** è responsabile del coordinamento operativo del **GSA** e della stesura dei rapporti sulle prestazioni del **GSA**
- Il **RGSA** implementerà programmi di formazione sulla sicurezza delle informazioni e di sensibilizzazione per i dipendenti
- la protezione dell'integrità, della disponibilità e della riservatezza delle attività è responsabilità del titolare di ogni risorsa
- tutti gli incidenti o i punti deboli della sicurezza devono essere segnalati a **RGSA**.

- **RGSA** definirà quali informazioni relative alla sicurezza delle informazioni saranno comunicate a quale parte interessata (sia interna che esterna), da chi e quando
- **RGSA** è responsabile dell'adozione e dell'implementazione del **Piano di Formazione e Sensibilizzazione**, che si applica a tutte le persone che hanno un ruolo nella gestione della sicurezza delle informazioni

## 4.5 Comunicazione della politica

**RGSA** si assicura che i dipendenti di Olomedia, oltre alle parti interessate pertinenti, abbiano familiarità con questa Politica; la stessa è pubblicata sul sito aziendale ([www.olomedia.it](http://www.olomedia.it)).

## 5 Supporto nell'implementazione del GSA

Con la presente la **DIR** dichiara che l'implementazione del **GSA** e il miglioramento continuo nella gestione della sicurezza delle informazioni saranno supportati con risorse adeguate al fine di raggiungere tutti gli obiettivi stabiliti in questa politica e a quelli identificati periodicamente, stanziando ad ogni riesame della direzione (annuale) una percentuale del fatturato annuo precedente in sicurezza per adeguamento della struttura e delle risorse umane. La **DIR** ha designato un **amministratore di sistema** che ha il compito di progettare, pianificare, e agire per garantire la che la sicurezza delle informazioni sia implementata come richiesto e stia raggiungendo i risultati attesi. La **DIR** si assicura che siano redatti e messa in pratica un piano di formazione per gli utenti, una politica di controllo degli accessi, un Piano di trattamento del rischio, il processo di trattamento del rischio ed una politica di Backup.

## 6 Validità e responsabilità della politica

Questa politica ha effetto dalla data dell'ultima emissione riportata sul frontespizio. Il responsabile della politica deve controllare e, se necessario aggiornare il documento con frequenza semestrale. Di seguito la matrice delle funzioni responsabili connesse alla presente politica. Durante la valutazione dell'efficacia e adeguatezza di questo documento, devono essere tenuti in considerazione i seguenti criteri:

- Num. impiegati e delle parti esterne che hanno un ruolo all'interno del **GSA**, ma non hanno familiarità con questo documento
- Non conformità del **GSA** alle leggi e i regolamenti, gli obblighi contrattuali e altri documenti interni dell'organizzazione
- Mancanza di efficacia dell'implementazione e mantenimento del **GSA**
- Responsabilità non chiare per l'implementazione del **GSA**

### R. Responsabile C. Collaboratore

|                    | <b>Soggetti responsabili</b> |           |            |
|--------------------|------------------------------|-----------|------------|
| Politica           | <b>DIR</b>                   | <b>RQ</b> | <b>RDP</b> |
| Redazione/Modifica |                              | <b>R</b>  |            |
| Verifica           |                              | <b>R</b>  |            |

|              |   |   |   |
|--------------|---|---|---|
| Approvazione | R |   |   |
| Attuazione   |   | R | C |