la lucente spa®

# Politica
# Sicurezza delle Informazioni

# Sicurezza delle informazioni

Il Consiglio di Amministrazione de La Lucente S.p.A. ("**Lucente**"), consapevole che le informazioni costituiscono un asset strategico fondamentale, definisce la presente Politica per garantire la protezione del proprio patrimonio informativo e la tutela della proprietà intellettuale. Essa rappresenta l'impegno a preservare i pilastri della sicurezza — Riservatezza, Integrità e Disponibilità — e ad assicurare la piena *compliance* normativa e contrattuale.

**Principi Guida**

**1. Tutela del Patrimonio Informativo e Conformità (CIA & GDPR)**

Lucente considera la sicurezza un fattore irrinunciabile per il business, impegnandosi a:

a. garantire la salvaguardia delle informazioni aziendali e di quelle affidate dai Clienti adottando i requisiti di controllo definiti dalla norma ISO/IEC 27001 e assicurando la piena conformità al Regolamento UE 679/2016 (GDPR);
b. proteggere gli asset informativi assicurandone la Riservatezza (accesso ai soli autorizzati), l'Integrità (accuratezza e completezza) e la Disponibilità (accessibilità al bisogno), prevenendo furti, alterazioni o interruzioni di servizio;
c. tutelare la proprietà intellettuale dei prodotti aziendali e le informazioni riservate, consolidando la percezione di affidabilità e fiducia da parte dei Clienti.

**2. Governance dei Rischi e Modello Organizzativo**

Lucente adotta un approccio preventivo e strutturato alla gestione delle minacce, attraverso:

a. l'adozione di un modello di **governance centralizzata** che esplicita chiare responsabilità nella gestione della sicurezza;
b. l'applicazione di una **metodologia quantitativa** per la gestione dei rischi, comprensiva di criteri oggettivi per l'accettazione degli stessi, supportata da un efficace meccanismo di valutazione periodica;
c. la scelta di controlli procedurali, tecnologici e organizzativi specifici per mitigare i rischi e prevenire prestazioni non conformi ai requisiti di servizio.

**3. Monitoraggio, Gestione Incidenti e Cultura**

Lucente promuove la resilienza operativa e la consapevolezza, impegnandosi a:

a. monitorare e analizzare continuativamente gli eventi di sicurezza per intercettare potenziali minacce prima che causino danni;
b. istituire meccanismi efficaci di reazione e gestione degli incidenti di sicurezza, inclusi i *data breach* di dati personali, per minimizzarne l'impatto;
c. garantire i risultati aziendali attraverso la partecipazione attiva e attenta del personale, promuovendo una cultura della cyber-security diffusa a tutti i livelli.

**Impegno della Direzione**
La Direzione si impegna a diffondere la presente Politica a tutti i livelli dell'organizzazione, assicurando che sia compresa, condivisa e attuata, e a riesaminarla periodicamente per accertarne la continua idoneità.

**Ambito di applicazione**
La Politica si applica a Lucente e a tutte le sue sedi operative e dipendenti ed è redatta dal team di sostenibilità interno. Una volta redatta è approvata dal Consiglio di Amministrazione della Società ed applicata congiuntamente alle altre policy adottate dalla Società.

**1. Tutela del Patrimonio Informativo e Conformità (CIA & GDPR)**

| Aspetto | Obiettivo | Indicatore di Performance (KPI) |
|---|---|---|
| **Riservatezza** | Protezione dei dati critici: Mantenere la riservatezza delle informazioni sensibili | Numero di incidenti di data breach |
| | Gestione degli accessi: garantire l'accesso solo al personale autorizzato e necessario | Account utente con privilegi |
| **Integrità** | Affidabilità dei dati: garantire l'accuratezza e la completezza delle informazioni | Tasso di successo dei controlli di integrità dei dati critici |
| | Controllo delle modifiche: mantenere la tracciabilità e l'approvazione di tutte le modifiche ai sistemi | Percentuale di modifiche ai sistemi che hanno violato il processo di Change Management |
| **Disponibilità** | Continuità operativa: assicurare la disponibilità dei servizi critici per il business | Tempo di Attività (Uptime) dei sistemi critici |
| | Capacità di ripristino: essere in grado di ripristinare i servizi rapidamente dopo un disastro | Tempo Medio di Ripristino (MTTR - Mean Time To Recover) dopo un incidente grave |

## 2. Governance dei Rischi e Modello Organizzativo

| Aspetto | Obiettivo | Indicatore di Performance (KPI) |
|---|---|---|
| **Gestione Rischi** | Riduzione del Rischio: diminuire l'esposizione complessiva ai rischi di sicurezza | Percentuale di Rischi di Livello "Alto" o "Critico" mitigati |
| **Efficacia SGSI** | Miglioramento Continuo: risolvere prontamente le non conformità e le debolezze | Percentuale di Azioni Correttive/Preventive completate in tempo |
| | Conformità e Audit: mantenere un elevato livello di conformità ai requisiti normativi e interni | Numero di Non Conformità "Maggiori" rilevate negli Audit Interni/Esterni |
| **Consapevolezza** | Fattore Umano: migliorare la consapevolezza della sicurezza tra tutti i dipendenti | Percentuale di Dipendenti che superano il test di formazione sulla sicurezza (es. phishing simulation) |
| | | Frequenza di partecipazione alla formazione obbligatoria sulla sicurezza |

## 3. Monitoraggio, Gestione Incidenti e Cultura

| Aspetto | Obiettivo | Indicatore di Performance (KPI) |
|---|---|---|
| **Incident Management** | Risposta agli Incidenti: gestire e risolvere gli incidenti di sicurezza in modo rapido ed efficace | Tempo Medio di Risposta (MTTD - Mean Time To Detect) a un incidente di sicurezza |
| | | Tempo Medio di Contenimento (Containment) dell'incidente |

la lucente spa®

# Policy
# Information Security

# Information Security

The Board of Directors of La Lucente S.p.A. ("**Lucente**"), aware that information is a fundamental strategic asset, has defined this Policy to ensure the protection of its information assets and intellectual property. It represents a commitment to preserving the pillars of security — Confidentiality, Integrity and Availability — and to ensuring full regulatory and contractual compliance.

## Guiding Principles

### 1. Information Asset Protection and Compliance (CIA & GDPR)

Lucente considers security to be an essential factor for business, committing itself to:

a. guaranteeing the protection of company information and information entrusted by customers by adopting the control requirements defined by ISO/IEC 27001 and ensuring full compliance with EU Regulation 679/2016 (GDPR);
b. protecting information assets by ensuring their confidentiality (access only to authorised persons), integrity (accuracy and completeness) and availability (accessibility when needed), preventing theft, alteration or service interruptions;
c. protect the intellectual property of company products and confidential information, consolidating the perception of reliability and trust on the part of customers.

### 2. Risk Governance and Organisational Model

Lucente adopts a preventive and structured approach to threat management through:

a. the adoption of a **centralised governance** model that sets out clear responsibilities in security management;
b. applying a **quantitative methodology** for risk management, including objective criteria for risk acceptance, supported by an effective periodic assessment mechanism;
c. choosing specific procedural, technological and organisational controls to mitigate risks and prevent performance that does not comply with service requirements.

### 3. Monitoring, Incident Management and Culture

Lucente promotes operational resilience and awareness, committing to:

a. continuously monitor and analyse security events to intercept potential threats before they cause damage;
b. establish effective mechanisms for responding to and managing security incidents, including personal data breaches, to minimise their impact;
c. ensuring business results through the active and attentive participation of

staff, promoting a culture of cyber security at all levels.

**Management Commitment**
Management is committed to disseminating this Policy throughout all levels of the organisation, ensuring that it is understood, shared and implemented, and to reviewing it periodically to ensure its continued suitability.

**Scope**
The Policy applies to Lucente and all its operating sites and employees and is drafted by the internal sustainability team. Once drafted, it is approved by the Company's Board of Directors and applied in conjunction with the other policies adopted by the Company.

**1. Information Asset Protection and Compliance (CIA & GDPR)**

| Aspect | Objective | Key Performance Indicator (KPI) |
|---|---|---|
| **Confidentiality** | Critical data protection: Maintaining the confidentiality of sensitive information | Number of data breach incidents |
| | Access management: ensuring access only to authorised and necessary personnel | Privileged user accounts |
| **Integrity** | Data reliability: ensuring the accuracy and completeness of information | Success rate of critical data integrity checks |
| | Change control: maintaining traceability and approval of all changes to systems | % of changes to systems that violated the Change Management process |
| **Availability** | Business continuity: ensuring the availability of critical services for the business | Uptime of critical systems |
| | Recovery capability: being able to restore services quickly after a disaster | Mean Time To Recover (MTTR) after a serious incident |

## 2. Risk Management and Organisational Model

| Aspect | Objective | Key Performance Indicator (KPI) |
|---|---|---|
| **Risk Management** | Risk Reduction: decreasing overall exposure to security risks | %of 'High' or 'Critical' Level Risks Mitigated |
| **SGSI effectiveness** | Continuous Improvement: promptly resolve non-conformities and weaknesses | % of Corrective/Preventive Actions completed on time |
| | Compliance and Auditing: maintaining a high level of compliance with regulatory and internal requirements | Number of 'Major' Non-Conformities identified in Internal/External Audits |
| **Awareness** | Human Factor: improving safety awareness among all employees | % of employees who pass the security training test (e.g., phishing simulation) |
| | | Frequency of attendance at compulsory safety training |

## 3. Monitoring, Incident Management, and Culture

| Aspect | Objective | Key Performance Indicator (KPI) |
|---|---|---|
| **Incident Management** | Incident Response: managing and resolving security incidents quickly and effectively | Mean Time To Detect (MTTD) for a security incident<br><br>Average incident containment time |