

## POLITICA DI SICUREZZA

### Sistema di Gestione per la Sicurezza delle Informazioni

#### Kirey Group

##### Storicità del documento

| Major Release | Azione      | Funzione Aziendale | Data       |
|---------------|-------------|--------------------|------------|
| 1             | Redatto     | CISO, ORG          | 28/06/2022 |
|               | Controllato | ORG                | 28/06/2022 |
|               | Pubblicato  | ORG                | 28/06/2022 |
|               |             |                    |            |

##### Storico delle modifiche

| Major Release | Minor Release | Data di pubblicazione | Motivo della revisione  |
|---------------|---------------|-----------------------|---|
| 1             | 0             | 27/04/2021            | Prima definizione in bozza  |
| 1             | 1             | 29/04/2021            | Aggiornamento e revisione del documento                             |
| 1             | 2             | 08/06/2021            | Revisione legal entity di riferimento                               |
| 1             | 3             | 06/09/2021            | Personalizzazione della politica per Kirey S.r.l.                   |
| 1             | 4             | 01/12/2021            | Integrazione legal entity e aggiornamento                           |
| 1             | 5             | 28/06/2022            | Aggiornamento dei ruoli coinvolti nella redazione del documento     |
| 1             | 6             | 09/05/2023            | Aggiornamento Struttura e Cambio tipologia documento in Linea Guida |

## **SOMMARIO**

|   |   |
|---|---|
| 1. OBIETTIVO .....                              | 3 |
| 2. DEFINIZIONI ED ACRONIMI.....                 | 3 |
| 2.1. Definizioni.....                           | 3 |
| <b>2.2. Acronimi</b> .....                      | 3 |
| 3. LINEE GUIDA SULLA POLITICA DI SICUREZZA..... | 3 |
| 3.1. Politica di Sicurezza .....                | 3 |
| 3.1.1. Premessa .....                           | 3 |
| 3.1.2. Significato ed Obiettivi .....           | 4 |
| 4. RIFERIMENTI.....                             | 4 |
| 5. ALLEGATI.....                                | 5 |

## 1. OBIETTIVO

Scopo del presente documento è definire i principi generali per la sicurezza delle informazioni cui attenersi per la realizzazione e il mantenimento di un efficiente e sicuro Sistema di Gestione per la Sicurezza delle Informazioni nell'ambito delle attività svolte da Kirey Group.

Questo documento si applica alle business line in perimetro di Kirey Group, secondo quanto specificato nel documento *PKG\_CIS\_RE01\_Perimetro ISMS*.

Il documento è 'pubblico', destinato a tutte le parti interessate dalle attività di Kirey Group.

## 2. DEFINIZIONI ED ACRONIMI

### 2.1. Definizioni

Si indicano i principali termini di riferimento ed acronimi utilizzati nel documento.

| Termine               | Descrizione   |
|-----------------------|---|
| <b>Riservatezza:</b>  | Assicura che l'informazione sia accessibile unicamente dal personale autorizzato                          |
| <b>Integrità:</b>     | Assicura che l'informazione sia accurata e completa   |
| <b>Disponibilità:</b> | Assicura che l'informazione sia accessibile ed utilizzabile, quando necessario, dal personale autorizzato |
|                       |   |

### 2.2. Acronimi

| Acronimo | Definizione                                    |
|----------|--|
| ISMS     | Information Security Management System         |
| ISO      | International Organization for Standardization |
| CISO     | Chief Information Security Officer             |

## 3. LINEE GUIDA SULLA POLITICA DI SICUREZZA

### 3.1. Politica di Sicurezza

#### 3.1.1. Premessa

Il Sistema di Gestione della Sicurezza delle Informazioni è lo strumento con il quale Kirey Group intende proteggere la riservatezza, l'integrità e la disponibilità del proprio patrimonio informativo. Il raggiungimento di adeguati livelli di sicurezza, consente di mitigare e contrastare perdite e il verificarsi di danni che possono avere impatto sulle persone, sull'operatività, sull'immagine e la reputazione aziendali, sugli aspetti di natura economica e finanziaria e sulle tecnologie, oltre a consentire la conformità al contesto contrattuale e legislativo vigente in materia di Protezione dei dati personali e delle informazioni.

A tal fine Kirey Group:

- adotta ed implementa principi e best practice riconosciuti per garantire la Sicurezza delle Informazioni e promuovono l'acquisizione di certificazioni di conformità agli standard di riferimento;
- individua ruoli e responsabilità, assegnati al proprio organico, indipendentemente dal livello gerarchico occupato, coinvolgendo anche i soggetti terzi che svolgono incarichi chiave;
- assegna le risorse necessarie al fine di assicurare l'impiego di misure di sicurezza adeguate per le informazioni, nel campo della sicurezza organizzativa, fisica e dei sistemi informativi, nell'erogazione dei processi di implementazione di soluzioni, anche di tipo applicativo, nella gestione e manutenzione di infrastrutture informatiche;
- promuove continuamente il Sistema di Gestione, anche mediante un impegno costante degli Organi e dei Soggetti apicali;
- individua, documenta ed applica regole che disciplinano le modalità di utilizzo delle informazioni, dei beni e degli strumenti, al fine di soddisfare la normativa vigente e le aspettative della clientela, principalmente di origine bancaria, finanziaria e della pubblica amministrazione, in osservazione alle necessità emergenti dalle relazioni e dalle dipendenze con altri processi delle Organizzazioni;
- sviluppa un programma di consapevolezza per il personale in materia di sicurezza, mediante sessioni informative e formative periodiche;
- predispone adeguate misure di reazione e gestione a fronte del verificarsi di incidenti che possono compromettere la sicurezza delle informazioni e la normale operatività;
- si impegna a svolgere un processo continuo di miglioramento ed evoluzione del Sistema di Gestione, pianificando, eseguendo, verificando e attuando con continuità misure ed accorgimenti atti a contrastare eventi che possano compromettere il patrimonio informativo aziendale.

### 3.1.2. Significato ed Obiettivi

La Sicurezza delle Informazioni ha come obiettivo primario la protezione delle informazioni, dei dati e degli elementi del sistema informativo che si occupano della loro gestione. In particolare, perseguire la sicurezza delle informazioni significa definire, conseguire e mantenere almeno le seguenti proprietà:

- **Riservatezza**
- **Integrità**
- **Disponibilità**

La mancanza di commisurati livelli di sicurezza, in termini di riservatezza, disponibilità e integrità delle informazioni, può comportare, nell'ambito di una qualsiasi attività di Kirey Group, perdita di reputazione, disaffezione della clientela, danni di natura economica e finanziaria, oltre a sanzioni penali e amministrative in seguito a violazione della normativa vigente.

## 4. RIFERIMENTI

Si indicano i documenti, le normative e gli standard utilizzati quale riferimento per la definizione del presente piano.

| Documenti di riferimento   |
|--|
| PKG_CIS_PR04_Gestione della Continuità Operativa                 |
| PKG_CIS_PR02_Procedura Gestione Incidenti Sicurezza Informazioni |
| PKG_HRE_AL07_Mansionario   |

|   |
|---|
| PKG_CIS_RE01_Perimetro ISMS   |
| ISO/IEC 27001:2013 - Information Security Management System – Requirements  |
| ISO/IEC 27002:2013 – Code of practice for Information Security Management   |
| ISO/IEC 27005:2018 – Information Security Risk Management   |
| ISO 22301:2019 – Societal Security – Business Continuity Management System – Requirements   |
| NIST – SP 800/53 - 2013 - Recommended security controls for federal information systems   |
| ISO/IEC 20000:2018 – Information Technology Service Management  |
| D.Lgs. n. 196/2003 - Codice in materia di protezione dei dati personali e provvedimenti successivi  |
| UE - Regolamento n. 679/2016 del Parlamento Europeo e del Consiglio   |
| D.Lgs. n. 231/2001 - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica |
| D.Lgs. n. 81/2008 - Tutela della salute e della sicurezza nei luoghi di lavoro  |
| Legge n. 300/1970 – Statuto dei lavoratori  |

## 5. ALLEGATI

Nessun Allegato