

## POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La ORION SrL considera essenziale la tutela della sicurezza delle informazioni che sono a qualunque titolo gestite dall'organizzazione e a tale l'azienda ha strutturato un sistema di gestione per la sicurezza delle informazioni prendendo a riferimento lo standard ISO/IEC 27001:2024. La sicurezza delle informazioni è basata sui seguenti requisiti fondamentali:

- **Riservatezza e diffusione controllata:** le informazioni devono essere accessibili solo a chi è debitamente autorizzato a prenderne visione e che ha una effettiva necessità di conoscere.
- **Integrità:** devono essere garantite l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione.
- **Disponibilità:** le informazioni devono essere fruibili e gli utenti autorizzati devono avere facilmente accesso alle informazioni e ai sistemi associati quando necessario. Inoltre le informazioni ritenute importanti o critiche dovranno essere accessibili anche in casi di emergenze, incidenti informatici o o altre situazioni non ordinarie.

La presente politica si applica a tutti i tipi di informazioni e in qualunque formato:

- **Informazioni personali:** questo tipo di informazioni dovrà essere trattato in conformità al regolamento europeo GDPR (Regolamento UE 2016/679)
- **Informazioni industriali:** informazioni di carattere commerciale, di prodotto, di progetto
- **Informazioni relative a terze parti** (clienti, fornitori, consulenti, partner) che hanno accesso, gestiscono o trattano informazioni di proprietà o in custodia di ORION SrL.

La presente Politica si applica a tutto il personale aziendale e ai collaboratori dell'organizzazione stessa. Inoltre la presente Politica stabilisce il quadro entro cui l'organizzazione stabilisce i propri obiettivi per la sicurezza delle informazioni e le procedure da seguire per la gestione.

La Direzione della ORION S.r.L. ha stabilito in particolare i seguenti obiettivi strategici

- **Valutazione dei rischi e revisione periodica della stessa** per identificare, valutare e trattare i rischi relativi alla sicurezza delle informazioni attraverso metodologie strutturate, riducendo l'esposizione alle minacce di compromissione a livelli accettabili.
- **Continuità Operativa:** dovrà essere garantita la resilienza dei sistemi e la business continuity a fronte di incidenti informatici, emergenze e analizzando e mitigando i rischi derivanti dagli scenari possibili, inclusi i fattori ed eventi climatici estremi sulla continuità delle infrastrutture tecnologiche e fisiche
- **Conformità legislativa:** piena ottemperanza ai requisiti di legge vigenti, inclusi il **GDPR** (Regolamento UE 2016/679) e la normativa europea NIS2 (direttiva UE 2022/2555).
- **Conformità contrattuale:** piena ottemperanza ai requisiti contrattuali e agli impegni contratti con i clienti e con altre terze parti in genere.

- **Consapevolezza del personale:** promuovere la cultura della sicurezza delle informazioni attraverso programmi continui di formazione e addestramento per ridurre il rischio legato al fattore umano.

Per il raggiungimento degli obiettivi, il funzionamento della gestione della sicurezza e per il miglioramento l'azienda si impegna a implementare dei controlli quali Controlli Organizzativi, Controlli sulle Persone, Controlli Fisici, Controlli Tecnologici.

La Direzione si impegna a stanziare le risorse necessarie, umane, economiche e strumentali per raggiungere gli obiettivi e mantenere attivo il sistema di gestione della sicurezza delle informazioni in un'ottica di miglioramento continuo. La Direzione si impegna ad assegnare ruoli, mansioni e responsabilità relativi alla sicurezza delle informazioni per adempiere agli obblighi derivanti dalla normativa e per garantire il funzionamento del sistema di gestione. Tutto il Personale è tenuto a rispettare le procedure operative derivate da questa Politica, oltre agli obblighi derivati dalle leggi applicabili.

La presente Politica è comunicata in azienda a tutto il personale e alle parti interessate. Sarà inoltre riesaminata periodicamente per valutarne la rispondenza alla normativa applicabile e all'operatività dell'organizzazione.

La Direzione

