DICHIARAZIONE GENERALE DI POLITICA PER LA SICUREZZA

Premessa

COMMON NET nasce dall'interesse e la volontà dei soci di applicare, in ambito aziendale, le competenze acquisite durante il percorso di studi e di ricerca universitario. I soci sono impegnati in prima persona nello sviluppo ed erogazione dei servizi dell'azienda.

Grazie alle competenze e all'esperienza maturata nel settore dell'Ingegneria Informatica e delle Telecomunicazioni e ad una costante attività di aggiornamento, COMMON NET ha sviluppato una infrastruttura fisica e logica indipendente attraverso cui offre, dal 2022, servizi cloud di tipo IaaS.

La Direzione di COMMON NET riconosce che la sicurezza delle informazioni è fondamentale per il successo e la reputazione della nostra azienda. I dati dei clienti, i risultati delle analisi, gli indirizzi suggeriti costituiscono informazioni il cui valore rappresenta il patrimonio aziendale, sia nostro che del cliente.

Politica

A tal fine, la Direzione si impegna a:

- **Proteggere la riservatezza, l'integrità e la disponibilità delle informazioni**
- **Implementare e mantenere un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) conforme alla norma ISO IEC 27001:2022 e secondo i controlli delle linee guida ISO IEC 27017:2015 e ISO IEC 27018:2019**
- **Fissare obiettivi di sicurezza per la riservatezza, l'integrità e la disponibilità delle informazioni**
- **Assicurare che tutti i dipendenti siano consapevoli delle loro responsabilità in materia di sicurezza delle informazioni**
- **Fornire le risorse necessarie per l'implementazione e il mantenimento del SGSI**
- **Migliorare continuamente il SGSI**

Impegno al Rispetto dei Requisiti

La Direzione e tutti i dipendenti si impegnano a rispettare tutti i requisiti previsti dalla norma ISO IEC 27001:2022. La Direzione si impegna a esercitare la leadership secondo quanto stabilito da tale norma.
La seguente **Politica Di Sicurezza** è stata sviluppata con l'obiettivo di fornire un quadro completo per la gestione della sicurezza delle informazioni nei servizi erogati dalla società. Questa politica si applica a tutti i dipendenti, i contractor e i terzi che hanno accesso alle informazioni dell'organizzazione.
Lo **scopo** di questa politica è quello di stabilire un framework per la protezione delle informazioni trattate nei servizi garantendo la loro riservatezza, integrità e disponibilità.

Politica appropriata alle finalità dell'organizzazione

Consapevoli che i dati del cliente costituiscono informazioni il cui valore rappresenta il patrimonio aziendale della nostra organizzazione e di quella del cliente, abbiamo implementato un sistema di gestione per la sicurezza delle informazioni prevedendo la messa a punto di tutti i controlli di sicurezza applicabili al trattamento delle informazioni.

Politica per fissare gli obiettivi di sicurezza

Grazie all'implementazione del sistema di gestione, abbiamo determinato gli obiettivi di sicurezza delle informazioni che ci vedranno impegnati, in ciascun processo aziendale, alla preservazione della:

- Riservatezza dei dati rilasciati dal cliente

- Integrità delle informazioni rilasciate dal cliente e quelle relative alle procedure di trattamento dei dati che impieghiamo per effettuare le analisi
- Disponibilità di tali informazioni alle persone autorizzate alla loro gestione e al loro impiego

Politica per l'impegno al rispetto dei requisiti applicabili

L'impegno della Direzione e di tutti coloro che a vario titolo sono coinvolti dalle attività del sistema di gestione è quello di rispettare tutti i requisiti previsti dalla Norma Internazionale ISO 27001:2022. Per questo, La Direzione assume l'impegno di esercitare la leadership secondo quanto stabilito da tale Norma.

Politica per l'impegno per il miglioramento continuo del sistema di gestione

Il patrimonio informativo del cliente e quello relativo al know-how della nostra organizzazione costituiranno d'ora innanzi i punti focali dell'impegno di tutti. Un impegno assunto da tutti e da ciascuno.

Tale impegno sarà manifestato attraverso le "performance di sicurezza" che dovranno dare evidenza di quanto la nostra organizzazione ed il nostro sistema di gestione della sicurezza delle informazioni siano efficaci nel registrare un miglioramento continuo. La politica è pubblicata sul sito internet dell'organizzazione.
Di seguito riportiamo il testo della Politica generale per la sicurezza delle informazioni, specificando che tale "Politica generale" si accompagna a politiche specifiche per argomento inserite nelle procedure per essere comunicate e sempre disponibili al personale che esegue le attività operative.

Il Campo di applicazione stabilito dall'Organizzazione è il seguente:

- **EROGAZIONE DI SERVIZI CLOUD DI TIPO IAAS. LE ATTIVITA' SONO STATE VERIFICATE SECONDO LE LINEE GUIDA ISO/IEC 27017:2015 E ISO/IEC 27018:2019.**

Miglioramento Continuo

La Direzione si impegna a migliorare continuamente il SGSI attraverso:

- **La revisione periodica del SGSI**
- **L'identificazione e la gestione dei rischi per la sicurezza delle informazioni**
- **L'implementazione di azioni correttive e preventive**
- **La formazione e la sensibilizzazione del personale sulla sicurezza delle informazioni**

Sulla base della ISO/IEC 27001:2022 la società attua e si impegna ad effettuare i seguenti controlli di sicurezza:

- **Gestione dei rischi:**

- Valutazione regolare dei rischi per la sicurezza delle informazioni e dei dati.
- Implementazione di misure di mitigazione dei rischi.

- **Gestione degli accessi:**

- Autenticazione a più fattori per l'accesso ai servizi.
- Autorizzazioni basate sui ruoli e sui principi del minimo privilegio.
- Monitoraggio delle attività degli utenti.

- **Crittografia:**

- Crittografia dei dati in transito e a riposo.
- Utilizzo di algoritmi crittografici forti e aggiornati.

- **Continuità operativa:**

- Piani di continuità operativa per garantire la disponibilità dei servizi in caso di incidenti.
- Test regolari dei piani di continuità operativa.

- **Gestione degli incidenti:**

- Procedure per la segnalazione, l'analisi e la gestione degli incidenti di sicurezza.
- Indagini approfondite sugli incidenti per individuare le cause e prevenire future occorrenze.

- **Privacy:**

- Protezione dei dati personali in conformità alle normative applicabili.
- Trasparenza nei confronti degli utenti riguardo all'utilizzo dei loro dati.

- **Governance:**

- Assegnazione di ruoli e responsabilità per la gestione della sicurezza delle informazioni.
- Revisione regolare della politica di sicurezza.

Conclusione

La Direzione è convinta che questa politica per la sicurezza delle informazioni sia fondamentale per il successo e la reputazione della nostra azienda. Ci impegniamo a fornire un ambiente sicuro e protetto per le informazioni dei nostri clienti e a migliorare continuamente il nostro SGSI.

Roma, 20 Novembre 2025 **La Direzione**