COMMON NET

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

MOD-520

DICHIARAZIONE GENERALE DI POLITICA PER LA SICUREZZA

La seguente **Politica Di Sicurezza** è stata sviluppata in conformità alle linee guida ISO/IEC 27001:2024 e alle relative estensioni ISO/IEC 27017:2015, ISO/IEC 27018:2019, con l'obiettivo di fornire un quadro completo per la gestione della sicurezza delle informazioni nei servizi cloud. 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 cloud, garantendo la loro riservatezza, integrità e disponibilità.

COMMON NET è un Internet Service Provider (ISP) che offre, attraverso infrastrutture di telecomunicazione di ultima generazione Wi-Fi e Fibra Ottica, servizi di connettività Internet in banda ultra larga.
Grazie alle competenze e all'esperienza maturata nel settore dell'Ingegneria Informatica e delle Telecomunicazioni e ad una costante attività di aggiornamento, COMMON NET offre servizi di consulenza e soluzioni all'avanguardia nell'ambito delle reti e dei sistemi informativi.

L'infrastruttura è costituita da risorse fisiche (hardware) chiamate "Compute Node", "Storage Node" e "Network Node" (nodi). I Compute Node contenegono la RAM e le CPU, i Storage Node contengono i dischi SSD mentre i Network Node contengono gli switch. Tali nodi sono installati all'interno di "Platform" (piattaforme) le quali forniscono l'alimentazione, la comunicazione e tutti i servizi di supporto. La rete presenta un'architettura Spine-Leaf dove ogni nodo di compute e di storage è collegato a due switch di livello Leaf.

Il servizio di virtualizzazione IaaS è erogato da Common Net è di tipo "Public Cloud". Tale servizio consente al Cliente di eseguire le proprie macchine virtuali (VMs) attraverso le risorse virtuali vRAM, vCPU e vDisk fornite da Common Net. Ogni VM è eseguita su di un compute node che fornisce 1:n ("1 compute node" : "n clienti") le risorse di vRAM e vCPU. Il vDisk è fornito attraverso un cluster HA (High Availability) distribuito dove i dati sono replicati su tre storage node differenti. Le risorse virtuali (pool) del Cliente sono organizzate in "tenant" ovvero istanze dedicate del servizio dove il Cliente può configurare e gestire le prorie VMs. La gestione del tenant avviene attraverso una interfaccia web a cui il Cliente può accedere con un Account fornito da Common Net.

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 del 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

COMMON NET

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

MOD-520

Politica per l'impegno al rispetto dei requisiti applicabili

L'impegno dell'alta 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 27001:2024. Per questo, l'alta 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.

CAMPO DI APPLICAZIONE: Questa politica si applica a tutte le informazioni trattate nei servizi cloud, inclusi i dati personali, i dati finanziari, i dati proprietari e le altre informazioni sensibili. Nello specifico l'organizzazione ha certificato i seguenti servizi:

PROGETTAZIONE, SVILUPPO, EROGAZIONE DI SERIVIZI CLOUD DI TIPO IAAS.

LE ATTIVITA' DI EROGAZIONE DI SERVIZI CLOUD DI TIPO IAAS SONO STATE IMPLEMENTATE ANCHE SECONDO LE LINEE GUIDA 27017:2016 E 27018:2019.

Politica per la Sicurezza delle Informazioni

Premessa

L'Alta 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, l'Alta 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 27001:2024 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, il mantenimento e il miglioramento del SGSI**

Obiettivi di Sicurezza

Gli obiettivi di sicurezza specifici includono:

- **Preservare la riservatezza dei dati rilasciati dal cliente**
- **Garantire l'integrità delle informazioni rilasciate dal cliente e quelle relative alle procedure di trattamento dei dati che impieghiamo per effettuare le analisi**
- **Assicurare la disponibilità di tali informazioni alle persone autorizzate alla loro gestione e al loro impiego**

Impegno al Rispetto dei Requisiti

L'Alta Direzione e tutti i dipendenti si impegnano a rispettare tutti i requisiti previsti dalla norma ISO/IEC 27001:2024. L'Alta Direzione si impegna a esercitare la leadership secondo quanto stabilito da tale norma.

Miglioramento Continuo

L'Alta 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**

COMMON NET

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

MOD-520

Sulla base della ISO IEC 27001:2024 e le estensioni 2017 e 2018 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 nel cloud.
– Implementazione di misure di mitigazione dei rischi.

- **Gestione degli accessi:**

– Autenticazione a più fattori per l'accesso ai servizi cloud.
– 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 cloud in caso di incidenti.
– Test regolari dei piani di continuità operativa.

- **Gestione delle incidenze:**

– 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 (es. GDPR).
– 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

L'Alta 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.

Data: 01/09/2024

Firma Direzione: