

Innovamat: Sicurezza e protezione dei dati

Indice dei contenuti

Iniziamo	3
Framework di sicurezza	4
La tua privacy è la nostra priorità	5
Gestione delle identità	5
Gestione dei programmi	5
Sicurezza degli endpoint	5
Sicurezza della posta elettronica	6
Sicurezza delle infrastrutture	6
Monitoraggio, registrazione e allerta del sistema	6
Conservazione ed eliminazione dei dati	7
Politiche di backup e disaster recovery	7
Gestione dei fornitori	7

Introduzione

Innovamat si assicura di proteggere i dati della comunità educativa a cui ha accesso. Per raggiungere questo obiettivo, adotta misure di sicurezza avanzate e garantisce la massima trasparenza nella gestione e nell'utilizzo dei dati, assicurandone il controllo e la protezione.

Framework di sicurezza

L'approccio alla sicurezza di Innovamat si basa su un modello di fiducia che garantisce una protezione completa dell'organizzazione e dei suoi dati a tutti i livelli. Il framework di sicurezza di Innovamat aderisce agli standard ISO 27001 e ENS e viene aggiornato con le indicazioni più recenti e le migliori pratiche del settore.

Innovamat gestisce e applica i protocolli con il supporto del team di sicurezza informatica, responsabile della sicurezza dell'informazione. Il team tecnico si occupa della progettazione di architetture di sviluppo sicure e dell'ingegneria della sicurezza, mentre il team legale gestisce i rischi e si assicura del rispetto della normativa di riferimento.

La tua privacy è la nostra priorità

L'approccio alla sicurezza di Innovamat è incentrato sulla protezione dei dati della comunità educativa attraverso misure di sicurezza avanzate. Il team di esperti in sicurezza, in collaborazione con i principali fornitori di cybersecurity, adotta le migliori metodologie e ricerca costantemente soluzioni innovative per potenziare i protocolli di sicurezza.

Il team tecnico di Innovamat ha sviluppato un solido ciclo di vita del software, integrando le migliori pratiche di sicurezza e rigorosi test in ogni fase, dal momento della progettazione iniziale fino all'implementazione e alla manutenzione. Questo approccio garantisce che tutti i prodotti siano realizzati con meticolosa attenzione alla sicurezza e al rispetto della normativa.

Gestione delle identità

- **Account utente**

A ogni account utente viene assegnato un identificatore unico. Tutti gli account utente sono protetti dall'autenticazione a due fattori, che fornisce un ulteriore livello di sicurezza per impedire l'accesso non autorizzato.

- **Diritti di accesso e accesso al sistema**

L'accesso è consentito esclusivamente previa autorizzazione esplicita e secondo il principio del minimo privilegio, con un registro dettagliato dei tentativi e degli accessi non riusciti.

- **Gestione delle password**

Innovamat richiede a tutto il personale l'uso di un sistema di gestione delle password per generare, archiviare e compilare automaticamente password complesse,

Gestione dei programmi

Innovamat utilizza software e applicazioni aziendali attentamente implementati e gestiti dal team IT interno. Garantisce che i dati delle applicazioni siano protetti e rimangano sicuri all'interno dell'organizzazione.

L'accesso alle applicazioni viene concesso in base al principio del minimo privilegio, con l'adozione costante di metodi di autenticazione sicuri. Inoltre, Innovamat protegge l'accesso a queste applicazioni attraverso specifiche politiche di sicurezza sui dispositivi endpoint.

Sicurezza degli endpoint

Tutte le stazioni di lavoro consegnate al personale di Innovamat sono configurate per rispettare le norme di sicurezza. Tali norme prevedono che le stazioni di lavoro siano configurate correttamente, aggiornate con regolarità e supervisionate continuamente tramite la soluzione di gestione degli endpoint di Innovamat. Per impostazione predefinita, le stazioni di lavoro sono configurate per crittografare il dispositivo di archiviazione, imporre l'uso di password sicure e bloccarsi automaticamente dopo un periodo di inattività. Inoltre, sono dotate di un antivirus di ultima generazione e di un software EDR (Endpoint Detection and Response) per rilevare e contrastare software dannosi, applicazioni non autorizzate e potenziali cyberattacchi.

prevenendo così il riutilizzo e riducendo il rischio di attacchi di phishing.

Tutti i dispositivi di proprietà dell'azienda e qualsiasi dispositivo personale utilizzato per accedere alle risorse aziendali sono soggetti alla soluzione di gestione dei dispositivi mobili di Innovamat.

Sicurezza della posta elettronica

La sicurezza della posta elettronica è cruciale per prevenire attacchi di furto di identità, phishing, ransomware e altro. Innovamat impiega misure di sicurezza avanzate per la posta elettronica, garantendo la protezione di tutte le comunicazioni. Queste misure comprendono l'adozione di avanzati filtri antispam, l'autenticazione multifattore e la crittografia delle e-mail che garantisce la protezione delle informazioni sensibili.

Innovamat utilizza sistemi avanzati di rilevamento delle minacce per identificare e bloccare le e-mail dannose prima che arrivino ai suoi dipendenti.

Innovamat organizza sessioni di formazione periodiche per aiutare il personale a riconoscere e notificare le e-mail sospette. Combinando queste strategie, Innovamat riduce significativamente il rischio di minacce via e-mail e garantisce l'integrità delle comunicazioni.

Sicurezza delle infrastrutture

Innovamat si avvale di fornitori esterni per l'erogazione dei servizi infrastrutturali, operando senza server o servizi locali.

I sistemi automatizzati aiutano a rilevare rapidamente qualsiasi problema potenziale

Di conseguenza, non è previsto alcun accesso esterno a una rete aziendale tradizionale.

Le applicazioni e i dati di Innovamat sono ospitati e protetti da una solida architettura di rete fornita dai principali fornitori di cloud pubblici. Questo approccio basato sul cloud garantisce una maggiore sicurezza, scalabilità e affidabilità.

Inoltre, Innovamat applica tecniche di rafforzamento dei server per aumentare la sicurezza dei server nel cloud. Queste misure includono aggiornamenti periodici, gestione delle patch, configurazioni di base e monitoraggio continuo per proteggere dalle vulnerabilità.

Utilizzando funzioni avanzate di sicurezza cloud e rigorose pratiche di rafforzamento dei server, Innovamat protegge le sue risorse e mantiene i più alti standard di protezione dei dati, garantendo che le operazioni siano allo stesso tempo efficienti e sicure.

Monitoraggio, registrazione e allerta del sistema

Innovamat monitora da vicino la sicurezza dei suoi server, delle stazioni di lavoro, dei dispositivi mobili e delle attrezzature di rete per mantenere una visione chiara e completa dell'infrastruttura aziendale e di produzione.

Innovamat registra e archivia i log degli accessi amministrativi, dei comandi privilegiati ed eventi del sistema in tutti i server e servizi di produzione.

e allertare il personale di sicurezza responsabile.

Conservazione ed eliminazione dei dati

Innovamat rispetta il GDPR, tratta i dati personali con il massimo rispetto della normativa vigente e offre ai suoi utenti il pieno controllo sulle loro informazioni.

I dati in possesso di Innovamat saranno conservati solo per il tempo strettamente necessario (ovvero, durante l'erogazione del servizio di accesso alla proposta formativa di Innovamat). Una volta terminato il rapporto, Innovamat procederà alla loro eliminazione.

Conserverà alcuni dati personali, identificativi e di traffico per un periodo massimo di 2 anni nel caso in cui ciò sia richiesto da Giudici e Tribunali o per avviare azioni interne derivanti da un uso improprio dell'app.

Per maggiori informazioni sulle politiche sulla privacy dei dati di Innovamat, consigliamo di consultare il Centro sulla privacy [qui](#).

Politiche di backup e disaster recovery

Attualmente, Innovamat crea backup degli asset e dei dati più critici, garantendone il ripristino anche in caso di eventi catastrofici.

Questo piano prevede la creazione di una copia delle informazioni critiche dall'attuale provider cloud e il loro trasferimento a un provider cloud alternativo.

Questa strategia mira a ridurre il rischio legato a potenziali attacchi informatici che potrebbero compromettere l'account principale del nostro provider cloud.

Gestione dei fornitori

Per operare in modo efficace, Innovamat si avvale di organizzazioni partner. Innovamat richiede ai partner di aderire agli standard e alle certificazioni di sicurezza del settore.

Stipula accordi che vincolano queste organizzazioni di servizi al rispetto degli impegni di riservatezza assunti nei confronti della sua comunità.

Innovamat riesamina l'efficacia dei partner di servizi prima della loro assunzione e successivamente almeno una volta all'anno.