DATA SHIELDS

SECURITY POLICY FOR THETA

www.datashields.tech

+025358985

info@datashields.com

Via della Sicurezza,20 Roma 00168

INTRODUZIONE

L’Azienda Theta si impegna a garantire la sicurezza e la protezione delle proprie risorse informatiche, delle informazioni aziendali e dei dati sensibili. Questa politica è progettata per minimizzare i rischi e proteggere l'azienda da potenziali minacce informatiche.

OBIETTIVI

- **Protezione dei dati:** Garantire che i dati aziendali e personali siano adeguatamente protetti contro accessi non autorizzati, furti, perdite e distruzioni.
- **Disponibilità dei servizi:** Assicurare che i sistemi informativi siano disponibili per gli utenti autorizzati quando necessario.
- **Integrità delle informazioni**: Assicurare che le informazioni siano accurate e affidabili e che non siano state alterate in modo non autorizzato.
- **Conformità**: Rispettare tutte le leggi, i regolamenti e le normative applicabili in materia di sicurezza informatica.

AMBITO DI APPLICAZIONE

Questa politica si applica a tutti i dipendenti, contrattisti, consulenti, temporanei e qualsiasi persona che abbia accesso ai sistemi informativi e alle risorse dell'Azienda Theta

RUOLI E RESPONSABILITA’

- **Direzione:**Fornire supporto e risorse per l'implementazione della politica di sicurezza.
- **Responsabile della Sicurezza Informatica (RSI)**:Supervisionare l'applicazione delle misure di sicurezza e la gestione degli incidenti.
- **Dipendenti**:Conformarsi alla politica di sicurezza e segnalare qualsiasi attività sospetta o incidente di sicurezza.
- **Fornitori e Terze Parti** :Devono rispettare le politiche di sicurezza di Theta e garantire la protezione delle informazioni a cui hanno accesso.

NORME E PROCEDURE

CONTROLLO DEGLI ACCESSI

- **Gestione degli account utente:**
  - Gli account utente sono creati solo per gli utenti autorizzati e devono essere revocati immediatamente al termine dell'autorizzazione.
  - Le password devono essere uniche, complesse (minimo 12 caratteri, con combinazione di lettere, numeri e simboli) e cambiate ogni 90 giorni.
- **Accesso remoto:**
  - L'accesso remoto ai sistemi aziendali deve essere autorizzato e protetto tramite VPN sicura.
  - È obbligatoria l'autenticazione a due fattori (2FA) per tutti gli accessi remotI.

PROTEZIONE DEI DATI

- **Criptazione:**
  - I dati sensibili devono essere criptati sia in transito che a riposo utilizzando algoritmi di crittografia robusti (ad es., AES-256).
- **Backup:**
  - Eseguire backup regolari dei dati critici e verificarne l'integrità. I backup devono essere conservati in una posizione sicura e devono essere testati periodicamente per garantire la loro ripristinabilità.
- **Classificazione dei dati:**
  - I dati devono essere classificati in base alla loro sensibilità (es., pubblico, riservato, confidenziale) e trattati di conseguenza.

GESTIONE DEGLI INCIDENTI

- **Segnalazione degli incidenti:**
  - Tutti gli incidenti di sicurezza devono essere segnalati immediatamente al RSI. Gli incidenti includono, ma non sono limitati a, violazioni dei dati, malware, tentativi di accesso non autorizzato.
- **Risposta agli incidenti:**
  - Il RSI deve avere un piano di risposta agli incidenti che includa la valutazione, la contenimento, la risoluzione e la comunicazione dell'incidente
- **Registro degli incidenti:****
  - Mantenere un registro aggiornato degli incidenti di sicurezza per l'analisi e la revisione.

UTILIZZO DELLE RISORSE INFORMATICHE

CONTROLLO DEGLI ACCESSI

- **Uso accettabile:**
  - Le risorse IT devono essere utilizzate esclusivamente per scopi aziendali. È vietato l'uso per attività personali non autorizzate o illegali.
- **Installazione del software:**
  - Solo il software autorizzato e licenziato può essere installato sui sistemi aziendali. Qualsiasi richiesta di installazione di software deve essere approvata dal dipartimento IT.

FORMAZIONE E CONSAPEVOLEZZA

- **Corsi di formazione:**
  - I dipendenti devono partecipare a corsi di formazione annuali sulla sicurezza informatica, inclusi moduli specifici su phishing, gestione delle password e protezione dei dati.
- **Campagne di sensibilizzazione:**
  - Devono essere promosse campagne di sensibilizzazione periodiche per aggiornare i dipendenti sulle minacce emergenti e sulle migliori pratiche di sicurezza.

PROTEZIONE DELLA RETE

- **Firewall e IDS:**
  - La rete aziendale deve essere protetta da firewall configurati correttamente e sistemi di rilevamento delle intrusioni (IDS).
- **Sicurezza Wi-Fi:**
  - Le reti Wi-Fi devono essere protette con crittografia WPA3 e accesso limitato solo a dispositivi aziendali autorizzati.

GESTIONE DEI RISCHI

- **Valutazione dei rischi:**
  - Devono essere effettuate valutazioni dei rischi annuali per identificare le vulnerabilità e le minacce alla sicurezza informatica.
- **Piani di mitigazione:**
  - Devono essere sviluppati piani di mitigazione per gestire e ridurre i rischi identificati.

CONFORMITA' LEGALE

- **Adempimenti normativi:**
  - L'azienda deve garantire la conformità con le leggi applicabili, inclusi GDPR, ISO 27001 e altre normative locali o internazionali rilevanti.
- **Audit di sicurezza:**
  - Devono essere condotti audit regolari per verificare la conformità alla politica di sicurezza e alle normative applicabili.

MONITORAGGIO E REVISIONE

Questa politica è stata approvata dalla Direzione dell'Azienda Theta e deve essere osservata da tutti i dipendenti e collaboratori.

Data di adozione: [Inserire data]
Data di revisione:[Inserire data di revisione]

Per ulteriori informazioni o chiarimenti, contattare il Responsabile della Sicurezza Informatica all'indirizzo [email del responsabile IT].

DATA_____

FIRMA_____