LE MISURE DI PROTEZIONE HP IN SINTESI

Per proteggere i dati dei clienti, HP applica una serie efficace di controlli per la protezione delle informazioni, tra cui politiche, pratiche, procedure e strutture organizzative per tutelare la riservatezza, l'integrità e la disponibilità delle informazioni dei propri clienti (inclusi i dati personali come definiti nelle appendici relative a clienti ed elaborazione dei dati di HP). Di seguito viene fornita una panoramica delle misure di protezione tecnico-organizzative di HP in tutta l'azienda.

1. Politica di protezione

   HP assicura politiche, standard e procedure applicabili a livello globale, volte a proteggere i dati di HP e dei clienti. Per proteggere l'integrità di dati e sistemi di HP, i dettagli sulle politiche di protezione HP sono riservati. Tuttavia, di seguito sono riepilogate le nostre politiche principali.

2. Organizzazione della protezione delle informazioni

   Il programma Information Security di HP è studiato per orientare e gestire la strategia e i controlli di protezione delle informazioni dell'organizzazione. Questo sistema garantisce la conformità alle politiche e ai controlli di sicurezza di HP, nonché il rispetto dei requisiti per la sicurezza dei clienti in tutta l'azienda. Questo Framework, che è strutturato in base ai framework di settore, alle leggi e ai regolamenti in materia di sicurezza informatica, viene rivisto ogni anno per essere adeguato allo scenario di minacce in continua evoluzione di HP.

3. Gestione dei rischi per la sicurezza informatica

   Il programma di gestione dei rischi per la sicurezza informatica di HP è progettato in modo da tutelare la riservatezza, l'integrità e la disponibilità delle informazioni. Questo programma fornisce un approccio uniforme per identificare, valutare, rendere o meno prioritari, gestire, rimediare a, monitorare e segnalare i rischi per la sicurezza informatica. HP definisce la propria Propensione al rischio come livello accettabile di esposizione a eventuali perdite e la Tolleranza del rischio come grado di scostamento da tale propensione. I rischi vengono valutati in base a una metodologia predefinita, che consente ad HP di contenere i rischi per la sicurezza delle informazioni a un livello accettabile. Questo programma è in linea con il processo di gestione aziendale dei rischi di HP.

4. Sicurezza HR

   La politica di sicurezza delle risorse umane di HP garantisce la protezione delle informazioni per tutto il periodo di permanenza dei dipendenti, istituendo processi per l'accesso a locali, sistemi informativi e altre risorse. Essa prevede, tra l'altro, l'acquisizione di consensi scritti tramite accordi di riservatezza e non divulgazione, nonché lo svolgimento di procedure di controllo delle esperienze pregresse. Tutti i candidati a posizioni HP devono sostenere un controllo di verifica delle esperienze pregresse in conformità alle leggi, ai regolamenti e ai codici etici applicabili.

5. Gestione delle risorse

   HP dispone di un processo per l'identificazione delle informazioni tecniche, la classificazione delle risorse critiche e lo svolgimento regolare di procedure di gestione documentate per ogni classe di informazioni, incluse quelle che comprendono Dati personali. Queste procedure riguardano l'archiviazione, la trasmissione e la comunicazione dei dati, l'accesso ai dati, la registrazione, la conservazione, la distruzione e l'eliminazione dei dati, la gestione degli incidenti e le notifiche di violazione dei dati. Le politiche e gli standard di protezione HP impongono inoltre lo smaltimento sicuro dei supporti.

6. Protezione dati

   Il programma di protezione dati di HP descrive le pratiche di sicurezza e i controlli tecnici che devono essere implementati per proteggere la privacy, l'autenticità e l'integrità dei dati. I requisiti legali, il valore, la criticità e la suscettibilità di divulgazione o modifica non autorizzate sono alcuni dei fattori che determinano il modo in cui le informazioni vengono classificate nell'ambito della politica di protezione dati di HP. Oltre alle procedure di gestione dei dati, questa politica descrive la crittografia, l'eliminazione, la raccolta, il trattamento, la conservazione, il backup e la prevenzione della perdita dei dati.

7. Controllo degli accessi

   HP adotta il principio dei privilegi minimi per il controllo degli accessi logici, fornendo l'accesso agli utenti tramite ID e password utente univoci. La politica per le password definisce i controlli di complessità, efficacia, validità e cronologia delle password. I diritti di accesso vengono rivisti periodicamente e vengono revocati al momento del congedo del personale. Vengono implementate procedure concordate per la creazione e l'eliminazione degli account utente al fine di concedere e revocare l'accesso ai sistemi client per la durata degli impegni.

8. Crittografia

   HP ha definito una serie di processi di crittografia efficaci per garantire la riservatezza, l'integrità e la disponibilità delle informazioni. I protocolli approvati prevedono la crittografia per alcune risorse, tra cui quelle contenenti dati personali. Il nostro programma di crittografia comporta l'utilizzo di tecniche matematiche per proteggere le informazioni e le comunicazioni, le quali fanno sì che solo le parti autorizzate possano accedere ai dati. Un componente essenziale del programma HP per la sicurezza delle informazioni è la protezione dei dati da accessi non autorizzati e manomissioni.

9. Sicurezza fisica e ambientale

   I locali di HP sono protetti da vari sistemi fisici ed elettronici di controllo degli accessi, compresi gli addetti alla sicurezza, il controllo elettronico degli accessi e le telecamere a circuito chiuso (TVCC). I locali sono anche dotati del necessario supporto alle infrastrutture, tra cui il controllo della temperatura e il backup dell'alimentazione tramite UPS e/o generatori diesel per supportare i servizi critici. Tutto il personale HP è registrato ed è tenuto a portare con sé badge identificativi idonei.

10. Gestione delle operazioni

    HP ha stabilito requisiti minimi per la protezione dell'infrastruttura tecnologica, tra cui workstation, server e apparecchiature di rete. Questi dispositivi utilizzano immagini di sistemi operativi precedentemente dotati di protezione avanzata, con requisiti variabili in base al sistema operativo e ai controlli implementati. Inoltre, HP ha sviluppato sistemi di rilevamento/prevenzione delle intrusioni di rete (NIDS/NIPS) che sono monitorati e gestiti 24 ore su 24, 7 giorni su 7.

11. Sicurezza delle comunicazioni

    La sicurezza delle comunicazioni garantisce la protezione delle informazioni all'interno delle reti aziendali. Essa prevede, tra l'altro, l'installazione e la gestione di componenti per la sicurezza di rete (come i firewall), l'isolamento delle reti, nonché il filtraggio web e i controlli per la gestione della posta elettronica. Inoltre, comporta il monitoraggio e la gestione dei canali di comunicazione per rilevare e prevenire accessi non autorizzati o violazioni dei dati.

12. Sicurezza dei sistemi

    La politica HP impone una metodologia per uno sviluppo sicuro dei sistemi e del software in tutte le sue fasi. Il ciclo di vita dello sviluppo software include le fasi iniziali, lo sviluppo/l'acquisizione, l'implementazione, l'utilizzo e la distruzione del software. Tutti i componenti del sistema vengono valutati in base al loro impatto sulla sicurezza complessiva. HP ha istituito controlli delle transazioni dei servizi applicativi, tra cui convalida delle credenziali utente, firme digitali, crittografia, protocolli di comunicazione protetti e archiviazione dei dettagli delle transazioni nell'area di rete protetta appropriata. Vengono inoltre eseguite analisi periodiche delle vulnerabilità interne.

13. Terzi e subappaltatori

    HP dispone di processi per la selezione di subappaltatori che soddisfino requisiti contrattuali di sicurezza omnicomprensivi. Per tutti i fornitori interessati che gestiscono dati di HP o di suoi clienti oppure l'accesso alla rete di HP, HP Cybersecurity conduce una valutazione del rischio allo scopo di valutare il relativo programma di protezione delle informazioni con misure fisiche, tecniche e amministrative. Questa valutazione è obbligatoria prima che il fornitore abbia accesso alle informazioni di HP.

14. Gestione di incidenti riguardanti la sicurezza delle informazioni

    HP dispone di un processo completo di gestione degli incidenti informatici che descrive finalità, ambito, ruoli, responsabilità, impegni di gestione, coordinamento organizzativo, procedure di implementazione e controlli di conformità. Questo processo viene rivisto e aggiornato ogni anno. Il Cyber Incident Response Team, che include personale addetto alla sicurezza informatica di HP addestrato nella risposta agli incidenti e nella gestione delle crisi, svolge analisi regolari del processo e di qualsiasi incidente o evento.

15. Gestione della continuità operativa

    Il programma globale per la continuità operativa di HP garantisce la continuità di tutte le operazioni attraverso processi di pianificazione collaborativi, standardizzati e documentati. L'azienda attua periodicamente i piani di continuità operativa per garantire l'efficacia, la verifica e l'aggiornamento di tutti i piani almeno una volta all'anno. Inoltre, tutto il personale coinvolto attivamente nel piano di continuità operativa riceve un'adeguata formazione.

16. Conformità

    La conformità informa l'approccio di HP al rispetto delle aspettative legali, contrattuali e interne di un programma efficace di sicurezza delle informazioni. Analisi regolari della sicurezza delle informazioni assicurano che i protocolli siano integrati nelle operazioni di ciascun gruppo aziendale. Questo processo di revisione garantisce inoltre l'aggiornamento della documentazione, in linea con gli obblighi legali man mano che i requisiti cambiano.

17. Settore delle carte di pagamento

    Il framework Payment Card Industry (PCI) guida l'approccio di HP al conseguimento della conformità PCI, descrivendo responsabilità aziendali e controlli di sicurezza conformi allo standard di sicurezza dei dati nel settore delle carte di pagamento (PCI DSS). Attraverso la creazione e il mantenimento di sistemi di controllo della sicurezza di rete, come i firewall, HP si accerta che la rete soddisfi i requisiti di conformità PCI.

18. Protezione prodotto HP

    La protezione prodotto HP comprende le pratiche fondamentali per la protezione dei prodotti HP, tra cui firma del codice, gestione delle vulnerabilità del prodotto, rilascio di bollettini sulla sicurezza e segnalazione dei problemi di sicurezza dei prodotti. Queste misure fanno in modo che i prodotti HP siano sempre sicuri e affidabili per gli utenti. La protezione prodotto è di fondamentale importanza in HP perché aiuta a conservare la fiducia dei clienti e protegge da potenziali minacce.

19. Sicurezza servizi HP

    La sicurezza servizi HP comprende pratiche fondamentali per proteggere i servizi forniti ai clienti HP. Questa politica affronta varie aree della sicurezza servizi come gli ambienti ospitati su infrastruttura HP e quelli ospitati da terze parti, dai partner e dai clienti. Queste misure garantiscono la sicurezza e l'affidabilità dei servizi HP per gli utenti. Attraverso l'implementazione di pratiche di protezione efficaci, HP garantisce la sicurezza e l'integrità dei propri prodotti e servizi, promuovendo un ambiente sicuro e affidabile per tutti gli utenti.