PŘEHLED BEZPEČNOSTNÍCH OPATŘENÍ SPOLEČNOSTI HP

Za účelem ochrany údajů zákazníků společnost HP dodržuje robustní soubor kontrolních mechanismů pro zabezpečení údajů, včetně zásad, praktik, postupů a organizačních struktur, aby zajistila důvěrnost, integritu a dostupnost svých vlastních údajů a údajů svých zákazníků (včetně osobních údajů, jak jsou definovány v dodatcích společnosti HP o zákaznících a zpracování údajů). V následující části je uveden přehled technických a organizačních bezpečnostních opatření společnosti HP týkajících se celé společnosti.

1. Zásady zabezpečení

   Společnost HP udržuje celosvětově platné zásady, standardy a postupy určené k ochraně údajů společnosti HP a jejích zákazníků. Podrobnosti bezpečnostních zásad společnosti HP jsou důvěrné z důvodu ochrany integrity dat a systémů společnosti HP. Shrnutí našich klíčových zásad je však obsaženo níže.

2. Organizace pro zabezpečení informací

   Program zabezpečení informací společnosti HP je určen k řízení a udržování strategie a kontrolních mechanismů zabezpečení informací v organizaci. Tento systém zajišťuje v rámci celého podniku dodržování zásad zabezpečení a kontrolních mechanismů zabezpečení společnosti HP a také dodržování bezpečnostních požadavků zákazníků. Tento rámec je strukturován v souladu s průmyslovými standardy pro kybernetickou bezpečnost, zákony a předpisy a je každoročně revidován, aby se přizpůsobil vyvíjejícímu se prostředí hrozeb společnosti HP.

3. Řízení rizik v kyberprostoru

   Program řízení rizik v kyberprostoru společnosti HP je navržen tak, aby chránil důvěrnost, integritu a dostupnost jejích informačních aktiv. Tento program poskytuje konzistentní přístup k identifikaci, hodnocení, stanovení priorit, ošetření, nápravě, sledování a hlášení rizik v oblasti kybernetické bezpečnosti. Společnost HP definuje svoji ochotu k riziku jako přijatelnou úroveň expozice ztrát a toleranci rizika jako stupeň odchylky od této ochoty. Rizika jsou vyhodnocována pomocí definované metodiky, což společnosti HP umožňuje zmírnit rizika zabezpečení informací na přijatelnou úroveň. Tento program je v souladu s procesem řízení podnikových rizik společnosti HP.

4. Zabezpečení protokolu HR

   Zásady zabezpečení lidských zdrojů společnosti HP zajišťují bezpečnost informací v průběhu celého pracovního cyklu zaměstnance stanovením postupů pro přístup k zařízením, informačním systémům a dalším aktivům. To zahrnuje získávání písemných potvrzení prostřednictvím dohod o důvěrnosti a mlčenlivosti, jakož i provádění postupů prověřování. Všichni uchazeči o zaměstnání ve společnosti HP musí absolvovat bezpečnostní prověrku v souladu s příslušnými zákony, předpisy a etickými pravidly.

5. Správa aktiv

   Společnost HP má zavedený proces pro identifikaci technických informačních aktiv, kategorizaci kritických aktiv a udržování dokumentovaných postupů pro nakládání s každým typem klasifikace informací, včetně těch, které obsahují osobní údaje. Tyto postupy se týkají ukládání, přenosu, komunikace, přístupu, protokolování, uchovávání, ničení, likvidace, řízení incidentů a oznamování porušení pravidel a norem. Zásady zabezpečení a standardy společnosti HP rovněž řídí bezpečnou likvidaci médií.

6. Zabezpečení dat

   Program zabezpečení dat společnosti HP popisuje bezpečnostní postupy a technické kontroly, které musí být zavedeny za účelem ochrany důvěrnosti, pravosti a integrity dat. Právní požadavky, hodnota, kritičnost a citlivost na neoprávněné vyzrazení nebo změnu jsou jen některé z faktorů, které určují, jak jsou informace klasifikovány v rámci zásad zabezpečení údajů společnosti HP. Kromě postupů pro nakládání s údaji jsou v zásadách popsány postupy pro šifrování, mazání, shromažďování a zpracování, uchovávání, zálohování a prevenci ztráty údajů.

7. Řízení přístupu

   Společnost HP používá pro řízení logického přístupu princip minimálních oprávnění a poskytuje uživatelům přístup prostřednictvím jedinečných uživatelských ID a hesel. Zásady hesla definují složitost, sílu, platnost a kontrolu historie hesel. Přístupová práva jsou pravidelně kontrolována a po odchodu zaměstnanců se ruší. Ve společnosti jsou zavedené dohodnuté postupy pro vytváření a rušení uživatelských účtů za účelem udělování a rušení přístupu do klientských systémů v průběhu pracovních aktivit.

8. Kryptografie

   Společnost HP definovala sadu robustních procesů pro kryptografii, které zajišťují důvěrnost, integritu a dostupnost informačních aktiv. Schválené protokoly vyžadují šifrování pro určitá aktiva, včetně aktiv obsahujících osobní údaje. Náš program Kryptografie zahrnuje použití matematických technik k zabezpečení informací a komunikace, které zajišťují, že k datům mají přístup pouze oprávněné strany. Klíčovou součástí programu pro zabezpečení informací společnosti HP je ochrana údajů před neoprávněným přístupem a nedovolenými zásahy.

9. Fyzické zabezpečení a bezpečnost prostředí

   Zařízení společnosti HP jsou zabezpečena pomocí různých fyzických a elektronických kontrol přístupu, včetně ostrahy, elektronické kontroly přístupu a uzavřeného kamerového okruhu (CCTV). Zařízení jsou rovněž vybavena nezbytnou podporou infrastruktury, včetně regulace teploty a zálohování napájení pomocí UPS a/nebo dieselových generátorů pro podporu kritických služeb. Všichni zaměstnanci HP jsou registrováni a musí nosit příslušné identifikační odznaky.

10. Správa operací

    Společnost HP stanovila minimální požadavky na zabezpečení technologické infrastruktury, včetně pracovních stanic, serverů a síťových zařízení. Tato zařízení využívají předem připravené bitové kopie operačního systému, přičemž požadavky se liší podle operačního systému a implementovaných prvků. Společnost HP navíc nasadila systémy pro detekci a prevenci narušení sítě (NIDS/NIPS), které jsou nepřetržitě monitorovány a spravovány.

11. Zabezpečení komunikace

    Zabezpečení komunikace zajišťuje ochranu informací v rámci podnikových sítí. To zahrnuje instalaci a správu síťových bezpečnostních prvků (např. firewallů), oddělení sítí, jakož i kontrolu filtrování webu a zpracování e-mailů. Dále zahrnuje monitorování a správu komunikačních kanálů s cílem odhalit a zabránit neoprávněnému přístupu nebo narušení dat.

12. Zabezpečení systémů

    Zásady společnosti HP nařizují bezpečnou metodiku vývoje systémů a softwaru po celou dobu jejich životního cyklu. Životní cyklus vývoje softwaru zahrnuje zahájení, vývoj/akvizici, implementaci, provoz a likvidaci. Veškeré součásti systému jsou vyhodnocovány z důvodu dopadu na celkové zabezpečení. Společnost HP zavedla kontrolní mechanismy pro transakce aplikačních služeb, včetně ověřování pověření uživatele, digitálních podpisů, šifrování, bezpečných komunikačních protokolů a ukládání podrobností o transakcích v příslušné bezpečnostní zóně sítě. Pravidelně se také provádí interní skenování chyb zabezpečení.

13. Třetí strany a dodavatelé

    Společnost HP má zavedené postupy pro výběr subdodavatelů, kteří splňují komplexní smluvní bezpečnostní požadavky. U příslušných dodavatelů, kteří nakládají s daty společnosti HP nebo zákazníků nebo mají přístup k síti společnosti HP, provede bezpečnostní oddělení společnosti HP posouzení rizik pro ověření programu zabezpečení informací s fyzickými, technickými a administrativními ochrannými opatřeními. Toto posouzení je nezbytné pro umožnění přístupu pro dodavatele k informacím společnosti HP.

14. Správa incidentů týkajících se zabezpečení informací

    Společnost HP má zavedený komplexní proces řízení kybernetických incidentů, který popisuje účel, rozsah, role, odpovědnosti, závazky vedení, organizační koordinaci, prováděcí postupy a kontrolu dodržování předpisů. Tento proces je každoročně přezkoumáván a aktualizován. Tým pro reakci na kybernetické incidenty, jehož součástí jsou pracovníci oddělení kybernetického zabezpečení společnosti HP vyškolení v oblasti reakce na incidenty a krizového řízení, provádí pravidelné kontroly procesů a všech incidentů nebo událostí.

15. Správa kontinuity podnikání

    Globální program kontinuity provozu společnosti HP zajišťuje komplexní kontinuitu prostřednictvím společných, standardizovaných a dokumentovaných procesů plánování. Společnost pravidelně testuje své plány kontinuity provozu, aby zajistila jejich účinnost, a nejméně jednou ročně testuje a aktualizuje všechny své plány. Kromě toho jsou všichni pracovníci zapojení do plánu kontinuity podnikání řádně proškoleni.

16. Dodržování předpisů

    Dodržování předpisů formuje přístup společnosti HP k plnění právních, smluvních a interních očekávání týkajících se účinného programu zabezpečení informací. Pravidelné revize zabezpečení informací zajišťují, že jsou protokoly integrovány do operací každé obchodní skupiny. Proces revize navíc udržuje dokumenty aktualizované tak, aby odrážely aktuální právní povinnosti, jelikož právní požadavky se vyvíjejí.

17. Průmysl platebních karet

    Rámec průmysl platebních karet (PCI) určuje přístup společnosti HP k dosažení souladu s požadavky v oboru PCI a popisuje obchodní povinnosti a bezpečnostní kontroly v souladu se standardem zabezpečení dat (DSS) v oboru PCI. Instalací a údržbou kontrolních prvků zabezpečení sítě, jako jsou brány firewall, společnost HP zajišťuje splnění požadavků v oblasti dodržování předpisů v oboru PCI.

18. Zabezpečení produktů HP

    Zabezpečení produktů společnosti HP zahrnuje základní postupy pro zabezpečení produktů HP, jako je podepisování kódem, správa chyb zabezpečení produktů, vydávání zpravodajů zabezpečení a hlášení problémů se zabezpečením produktů. Tato opatření zajišťují, že produkty HP zůstávají pro uživatele bezpečné a spolehlivé. Zabezpečení produktů má ve společnosti HP zásadní význam, protože pomáhá udržet důvěru zákazníků a chrání před potenciálními hrozbami.

19. Zabezpečení služeb společnosti HP

    Zabezpečení služeb společnosti HP zahrnuje základní postupy pro zabezpečení služeb poskytovaných zákazníkům společnosti HP. Tyto zásady se týkají různých oblastí zabezpečení služeb, včetně prostředí hostovaných v infrastruktuře HP, hostovaných u třetích stran, hostovaných u partnerů a hostovaných u zákazníků. Tato opatření zajišťují, že služby HP zůstávají pro uživatele bezpečné a spolehlivé. Zavedením důkladných bezpečnostních postupů zajišťuje společnost HP bezpečnost a integritu svých produktů a služeb, čímž zajišťuje bezpečné a důvěryhodné prostředí pro všechny uživatele.