REZUMATUL MĂSURILOR DE SECURITATE HP

Pentru a proteja datele clienților, HP a implementat măsuri de securitate stricte, adică politici, practici, proceduri și structuri organizaționale, asigurând astfel confidențialitatea, integritatea și disponibilitatea informațiilor referitoare la clienții săi (inclusiv datele cu caracter personal, așa cum sunt definite în Actul adițional HP privind prelucrarea datelor clientului). Urmează prezentarea generală a măsurilor de securitate HP de natură tehnică/organizațională valabile pentru întreaga companie.

1. Politică de securitate

   HP deține politici, norme și proceduri menite să protejeze datele HP și pe cele ale clienților, valabile la nivel global. Pentru protejarea integrității datelor și sistemelor HP, detaliile politicilor de securitate HP sunt confidențiale. Prezentăm mai jos doar un rezumat al principalelor noastre politici.

2. Organizație de securitate informațională

   Programul HP Information Security (Securitate informațională) este conceput pentru direcționarea și menținerea strategiei și măsurilor de securitate informațională ale organizației. Acest sistem asigură conformitatea întregii companii cu politicile și măsurile de securitate ale HP, precum și respectarea cerințelor de securitate ale clienților săi. Fiind structurat conform normelor, legilor și regulamentelor de securitate standard din domeniu, sistemul este revizuit anual, pentru a se adapta amenințărilor în evoluție la adresa HP.

3. Managementul riscurilor de securitate cibernetică

   Programul HP de management al riscurilor de securitate cibernetică este conceput pentru a proteja confidențialitatea, integritatea și disponibilitatea activelor informaționale HP. Acesta cuprinde o abordare consecventă pentru identificarea, evaluarea, prioritizarea, tratarea, remedierea, urmărirea și raportarea riscurilor de securitate cibernetică. HP definește „apetitul la risc" ca nivelul acceptabil al expunerii la pierderi și „toleranța la risc" ca gradul de acceptare a riscului respectiv. Riscurile sunt evaluate printr-o metodologie bine stabilită, astfel încât HP să poată menține riscurile de securitate a informațiilor la un nivel acceptabil. Acest program este coordonat cu procesul HP de management al riscurilor.

4. Securitatea resurselor umane

   Politica HP privind securitatea resurselor umane asigură securitatea informațiilor angajaților pe întreaga perioadă de activitate, stabilind procese pentru accesul la unități, sisteme informatice și alte active. Acestea includ confirmarea în scris a acceptării acordurilor de confidențialitate și nedezvăluire, precum și proceduri de verificare a antecedentelor. Toți candidații pentru angajarea la HP trebuie să treacă prin procesul de verificare, conform legilor, reglementările și normelor de etică relevante.

5. Gestionarea activelor

   HP are un proces de identificare a activelor informaționale tehnice, activele esențiale fiind incluse într-o categorie separată, precum și proceduri de manipulare a informațiilor în funcție de clasificarea acestora, inclusiv a celor care conțin date cu caracter personal. Procedurile respective acoperă stocarea, transmiterea, comunicarea, accesul, conectarea, păstrarea, distrugerea, eliminarea, gestionarea incidentelor și notificările privind încălcările. Politicile și normele de securitate HP conțin și prevederi privind eliminarea securizată a suporturilor de date.

6. Securitatea datelor

   Programul HP Data Security (Securitatea datelor) indică practicile de securitate și măsurile de natură tehnică necesare pentru protejarea confidențialității, autenticității și integrității datelor. Legislația, valoarea, importanța și consecințele dezvăluirii sau modificării neautorizate a datelor sunt doar câțiva dintre factorii care determină modul de clasificare a informațiilor în cadrul politicii HP privind securitatea datelor. Pe lângă procedurile de manipulare a datelor, politica se referă și la criptarea, ștergerea, colectarea și prelucrarea, păstrarea, copierea și prevenirea pierderii datelor.

7. Controlul accesului

   HP utilizează principiul privilegiului minim pentru controlul logic al accesului, oferindu-le acces utilizatorilor prin ID-uri și parole unice. Politica pentru parole stabilește regulile privind complexitatea, puterea, validitatea și istoricul acestora. Drepturile de acces sunt revizuite periodic și revocate în cazul părăsirii companiei. Sunt implementate proceduri de creare și de ștergere a conturilor, pe care utilizatorii trebuie să le accepte pentru a obține acces la sisteme cât timp sunt angajați ai HP.

8. Criptografiere

   HP a stabilit procese clare privind criptografierea, pentru a asigura confidențialitatea, integritatea și disponibilitatea activelor informative. Conform protocoalelor aprobate, anumite active trebuie criptate, inclusiv cele care conțin date cu caracter personal. Programul nostru de criptografiere prevede utilizarea unor tehnici matematice pentru securizarea informațiilor și a comunicărilor asigurând faptul că datele pot fi accesate doar pe bază de autorizare. O componentă esențială a programului HP de securitate a informațiilor protejează datele împotriva accesării și modificării neautorizate.

9. Securitatea fizică și a mediului

   Accesul în sediile HP este securizat prin diferite mijloace fizice și electronice, care includ personalul de pază, controlul electronic al accesului și televiziunea cu circuit închis (CCTV). De asemenea, sediile dețin infrastructura auxiliară necesară, adică un sistem de control al temperaturii și surse de alimentare neîntreruptibile, cum ar fi UPS și/sau generatoarele cu motorină, pentru serviciile esențiale. Tot personalul HP este înregistrat și trebuie să poarte ecusonul de identificare corespunzător.

10. Managementul operațiunilor

    HP a stabilit cerințele minime pentru protecția infrastructurii tehnologice, adică a stațiilor de lucru, a serverelor și a echipamentelor de rețea. Aceste dispozitive utilizează sisteme de operare care au încorporate opțiuni de protecție, cerințele fiind diferite în funcție de sistemul de operare și de măsurile de control implementate. În plus, HP a implementat Sistemele de detectare/prevenire a pătrunderii în rețea (NIDS/NIPS), monitorizate și gestionate nonstop.

11. Securitatea comunicărilor

    Securitatea comunicărilor asigură protecția informațiilor transmise prin intermediul rețelelor corporative. Aceasta include instalarea și gestionarea unor componente de securitate a rețelei (de exemplu, a firewallurilor), separarea rețelelor, filtre pentru accesarea internetului și controlul utilizării e-mailului. În plus, presupune monitorizarea și gestionarea canalelor de comunicare, pentru a se detecta și preveni accesarea neautorizată sau încălcarea securității datelor.

12. Securitatea sistemelor

    Politica HP impune o metodologie de dezvoltare securizată pentru sisteme și software pe parcursul întregului ciclu de viață. Ciclul de viață al dezvoltării unui software cuprinde inițierea, dezvoltarea/achiziționarea, implementarea, utilizarea și eliminarea. Sunt evaluate toate componentele sistemului, pentru identificarea impactului lor asupra securității generale. HP a stabilit măsuri de protecție pentru tranzacțiile din cadrul aplicației, inclusiv validarea datelor de conectare ale utilizatorilor, semnăturile digitale, criptarea, protocoalele de comunicare securizată și stocarea detaliilor tranzacțiilor în zona de securitate a rețelei. De asemenea, se efectuează scanări periodice, pentru depistarea vulnerabilităților interne.

13. Terți și subcontractanți

    HP are procese pentru selectarea subcontractanților, aceștia trebuind să respecte cerințe contractuale stricte privind securitatea. În cazul furnizorilor care au acces la date ale HP sau ale clienților și la rețeaua HP, departamentul de securitate cibernetică HP efectuează o analiză de risc, verificând măsurile de protecție a informațiilor fizice, tehnice și administrative adoptate. Analiza este obligatorie înainte ca furnizorii să poată accesa orice informație HP.

14. Managementul incidentelor de securitate a informațiilor

    HP are un proces complet de management al incidentelor cibernetice, fiind descrise scopul, domeniul de aplicare, rolurile, responsabilitățile, implicarea conducerii, coordonarea la nivel de organizație, procedurile de implementare și verificarea conformității. Acest proces este revizuit și actualizat anual. Echipa de răspuns la incidentele cibernetice, care cuprinde și departamentul de securitate cibernetică al HP, cu personal instruit în gestionarea incidentelor și a situațiilor de criză, analizează periodic procesul respectiv și toate incidentele sau evenimentele.

15. Managementul continuității activității

    Programul pentru continuitatea activității HP la nivel global asigură continuitatea tuturor activităților prin procese de planificare colaborative, standardizate și documentate. Compania testează periodic planurile de continuitate a activității pentru a se asigura că sunt eficiente, actualizându-le pe toate cel puțin anual. În plus, tot personalul implicat în planul de continuitate a activității primește instruirea corespunzătoare.

16. Conformitate

    Conformitatea determină acțiunile HP în vederea îndeplinirii cerințelor legale, contractuale și interne privind deținerea unui program de securitate a informațiilor eficient. Revizuirea periodică a securității informațiilor asigură faptul că protocoalele sunt integrate în operațiunile fiecărui departament al companiei. Procesul de revizuire prevede și păstrarea documentelor actualizate, pentru reflectarea obligațiilor legale curente în cazul modificării cerințelor.

17. Industria cardurilor de plată

    Regulamentul privind cardurile de plată (PCI) determină modul în care acționează HP pentru a respecta PCI DSS (normele de securitate a datelor din industria cardurilor de plată), indicând responsabilitățile și măsurile de control ale companiilor. HP asigură respectarea cerințelor de conformitate cu PCI instalând și menținând măsuri de protecție a rețelei, precum firewallurile.

18. Securitatea produselor HP

    Securitatea produselor HP cuprinde metodele prin care sunt securizate produsele HP, cum ar fi semnarea codurilor, gestionarea vulnerabilităților de securitate, emiterea buletinelor de securitate și raportarea problemelor de securitate. Aceste măsuri asigură faptul că produsele HP sunt întotdeauna sigure și de încredere pentru utilizatori. Securitatea produselor are o importanță maximă pentru HP, deoarece contribuie la menținerea încrederii clienților și protejează împotriva amenințărilor potențiale.

19. Securitatea serviciilor HP

    Securitatea serviciilor HP cuprinde practici esențiale pentru securizarea serviciilor furnizate clienților HP. Această politică se referă la diferite aspecte ale securității serviciilor, adică la infrastructura găzduită de HP, de terți, de parteneri și de clienți. Măsurile respective asigură faptul că serviciile HP sunt întotdeauna sigure și de încredere pentru utilizatori. Prin implementarea unor practici de securitate robuste, HP asigură protecția și integritatea produselor și serviciilor sale, menținând un mediu sigur și de încredere pentru toți utilizatorii.