РЕЗЮМЕ НА МЕРКИТЕ ЗА СИГУРНОСТ НА HP

За да защити данните на Клиента, HP се придържа към надежден набор от контроли за информационна сигурност, включително политики, практики, процедури и организационни структури с цел запазване на поверителността, целостта и наличността на собствената си информация и информация на клиентите си (включително Лични данни, както е дефинирано в „Допълненията“ на HP за клиенти и обработване на данни). По-долу е даден преглед на техническите/организационните мерки за сигурност на HP в цялата компания.

1. Политика за осигуряване на сигурността

   HP поддържа глобално приложими правила, стандарти и процедури, предназначени да защитават данните на HP и на клиентите. Подробностите за политиките за осигуряване на сигурността на HP са поверителни, за да се защити целостта на данните и системите на HP. Обобщенията на основните ни политики обаче са включени по-долу.

2. Организация на информационната сигурност

   Програмата за информационна сигурност на HP има за цел да насочва и поддържа стратегията и контролите на организацията за информационна сигурност. Тази система гарантира съответствие в целия бизнес с политиките и контролите за сигурност на HP, както и придържане към изискванията за сигурност на своите клиенти. Рамката се преразглежда ежегодно, за да се адаптира към променящия се пейзаж на заплахите на HP, структурирана в съответствие със стандартните в отрасъла рамки, закони и разпоредби за киберсигурност.

3. Управление на риска в областта на киберсигурността

   Програмата на HP за управление на риска в областта на киберсигурността има за цел да запази поверителността, целостта и наличността на информационните си активи. Програмата предоставя последователен подход при идентифицирането, оценката, определянето на приоритетите, третирането, отстраняването, проследяването и отчитането на рисковете за киберсигурността. HP определя рисковия си апетит като приемливо ниво на изложеност на загуби, а рисковия толеранс — като степента на отклонение от този апетит. Рисковете се преценяват по дефинирана методика, като се дава възможност на HP да обезпечи рисковете за сигурността на информацията до приемливо ниво. Тази програма е съобразена с процеса Управление на корпоративния риск на HP.

4. Сигурност на ЧР

   Политиката на HP за сигурност на човешките ресурси гарантира сигурност на информацията през целия жизнен цикъл на заетите лица, като създава процеси за достъп до съоръжения, информационни системи и други активи. Това включва набавяне на писмени потвърждения чрез споразумения за поверителност и неразкриване на информация, както и провеждане на процедури за проверка на миналото. Всички кандидати за работа в HP трябва да преминат проверка на миналото в съответствие със съответните закони, наредби и етика.

5. Управление на активите

   HP има процес на идентифициране на техническите информационни активи, категоризиране на критичните активи и поддържане на документирани процедури за работа с всеки тип класификация на информацията, включително тези, съдържащи лични данни. Тези процедури покриват съхраняването, предаването, комуникацията, достъпа, регистрирането, задържането, унищожаването, изхвърлянето, управлението на инцидентите и уведомяването за нарушения. Политиките и стандартите за сигурност на HP също така задължават защитеното изхвърляне на носители.

6. Сигурност на данните

   Програмата HP за сигурност на данните набелязва практиките за сигурност и техническите контроли, които трябва да се прилагат, за да се защитят поверителността, автентичността и целостта на данните. Правните изисквания, стойност, критичност и чувствителност към неупълномощено разкриване или модификация са някои от факторите, които определят начина на класификация на информацията съгласно правилата на HP за сигурност на данните. Освен процедурите за обработка на данни, правилата очертават шифроването на данни, изтриването, събирането и обработването, задържането, архивирането и предотвратяването на загубата на данни.

7. Контрол на достъпа

   HP използва принципа на най-малко привилегии за контрол на логическия достъп, като предоставя достъп на потребителите чрез уникални потребителски идентификатори и пароли. Политиката за паролите определя контрол на сложността, силата, валидността и историята на паролите. Правата за достъп се преразглеждат периодично и се отнемат при напускане на персонала. Прилагат се съгласувани процедури за създаване и изтриване на потребителски акаунти за предоставяне и отнемане на достъп до клиентски системи по време на ангажименти.

8. Криптография

   HP е определила набор от надеждни процеси за криптография, за да гарантира поверителността, целостта и наличността на информационните активи. Одобрените протоколи изискват шифроване за определени активи, включително тези, които съдържат лични данни. Нашата програма за криптография включва използването на математически техники за защита на информацията и комуникациите, като се гарантира, че само упълномощени страни имат достъп до данните. Критичен компонент на програмата за информационна сигурност на HP е защитата на данните от неоторизиран достъп и подправяне.

9. Физическа и екологична сигурност

   Съоръженията на HP се защитават с използване на различни физически и електронни контроли за достъп, включително охранители, електронен контрол на достъпа и затворена телевизия (CCTV). Съоръженията са оборудвани и с необходимата инфраструктурна поддръжка, включително контрол на температурата и резервно захранване, като се използват UPS и/или дизелови генератори за поддръжка на критични услуги. Целият персонал на HP е регистриран и трябва да носи подходящи идентификационни знаци.

10. Управление на дейностите

    HP е установила минимални изисквания за укрепване на технологичната инфраструктура, включително работни станции, сървъри и мрежово оборудване. Тези устройства използват предварително подготвени образи на операционни системи, като изискванията варират в зависимост от операционната система и прилаганите контроли. Освен това HP е внедрила системи за откриване/предотвратяване на мрежови проникванията (NIDS/NIPS), които се наблюдават и управляват 24 часа в денонощието, 7 дни в седмицата.

11. Комуникационна сигурност

    Комуникационната сигурност осигурява защита на информацията в корпоративните мрежи. Това включва инсталиране и управление на компоненти за мрежова сигурност (напр. защитни стени), разделяне на мрежите, както и контрол на уеб филтрирането и обработката на електронна поща. Освен това включва наблюдение и управление на комуникационни канали с цел откриване и предотвратяване на неупълномощен достъп или пробив в данните.

12. Сигурност на системите

    Политиката на HP изисква методология за сигурна разработка на системи и софтуер през целия им жизнен цикъл. Жизненият цикъл на софтуера обхваща иницииране, разработване/придобиване, внедряване, експлоатация и изхвърляне. Оценява се въздействието на всички компоненти на системата върху цялостната сигурност. HP е въвела контроли за трансакциите на приложните услуги, включително валидиране на потребителските пълномощия, цифрови подписи, криптиране, сигурни протоколи за комуникация и съхраняване на данните за трансакциите в съответната зона за сигурност на мрежата. Извършват се и редовни вътрешни сканирания на уязвимостите.

13. Трети лица и подизпълнители

    HP има процеси за избор на подизпълнители, които отговарят на всеобхватни договорни изисквания за сигурност. За приложимите доставчици, които работят с данни на HP или клиенти или имат достъп до мрежата на HP, HP Cybersecurity извършва оценка на риска, за да провери програмата за информационна сигурност с физически, технически и административни предпазни мерки. Тази оценка се изисква, преди доставчикът да получи достъп до информацията на HP.

14. Управление на инциденти в областта на информационната сигурност

    HP разполага с цялостен процес за управление на киберинциденти, който очертава целта, обхвата, ролите, отговорностите, ангажираността на ръководството, организационната координация, процедурите за изпълнение и проверката за съответствие. Този процес се преразглежда и актуализира ежегодно. Екипът за реагиране при кибернетични инциденти, включващ служители на HP по киберсигурност, обучени в областта на реагирането при инциденти и управлението на кризи, извършва редовни настолни прегледи на процеса и на всички инциденти или събития.

15. Управление на непрекъсваемостта на дейността

    Глобалната програма за непрекъсваемост на операциите на HP осигурява непрекъсваемост от край до край чрез съвместни, стандартизирани и документирани процеси на планиране. Компанията периодично упражнява плановете си за непрекъсваемост на дейността, за да гарантира тяхната ефективност, като тества и актуализира всички планове поне веднъж годишно. Освен това целият персонал, участващ в плана за непрекъсваемост на дейността, получава подходящо обучение.

16. Съответствие

    Съответствието оформя подхода на HP за изпълнение на правните, договорните и вътрешните очаквания към ефективна програма за информационна сигурност. Редовните прегледи на информационната сигурност гарантират интегрирането на протоколите в операциите на всяка бизнес група. Процесът на преглед също така поддържа документите актуализирани, за да отразяват текущите правни задължения, тъй като изискванията се развиват.

17. Payment Card Industry (Индустрия за платежни карти)

    Рамката на Payment Card Industry (PCI) ръководи подхода на HP за постигане на съответствие с PCI, като очертава бизнес отговорностите и контролите за сигурност, съобразени с PCI DSS. Чрез инсталиране и поддържане на средства за контрол на мрежовата сигурност, като например защитни стени, HP гарантира, че отговаря на изискванията за съответствие с PCI.

18. Сигурност на продуктите на HP

    Сигурността на продуктите на HP обхваща основни практики за защита на продуктите на HP, като например подписване на код, управление на уязвимостите в сигурността на продуктите, издаване на бюлетини за сигурност и докладване на проблеми със сигурността на продуктите. Тези мерки гарантират, че продуктите на HP остават сигурни и надеждни за потребителите. Сигурността на продуктите е от първостепенно значение за HP, тъй като помага за поддържане на доверието на клиентите и предпазва от потенциални заплахи.

19. Сигурност на услугите на HP

    Сигурността на услугите на HP обхваща основни практики за защита на услугите, предоставяни на клиентите на HP. Тази политика се отнася до различни области на сигурността на услугите, включително среди, хоствани от инфраструктурата на HP, от трети страни, от партньори и от клиенти. Тези мерки гарантират, че услугите на HP остават сигурни и надеждни за потребителите. Чрез прилагането на надеждни практики за сигурност HP гарантира безопасността и целостта на своите продукти и услуги, като създава сигурна и надеждна среда за всички потребители.