КРАТКОЕ ОПИСАНИЕ МЕР БЕЗОПАСНОСТИ КОМПАНИИ HP

Для защиты данных клиентов компания HP реализует комплекс мер по обеспечению информационной безопасности, включая правила, политики, процедуры и организационные структуры, которые направлены на сохранение конфиденциальности, целостности и доступности как собственной информации компании HP, так и информации ее клиентов (включая персональные данные, определение которых содержится в дополнении, посвященном обработке данных клиентов компании HP). Ниже приводится обзор технических и организационных мер безопасности, предпринимаемых в компании HP.

1. Политика безопасности

   Компания HP по всему миру соблюдает политики, стандарты и процедуры, предназначенные для защиты данных компании HP и ее клиентов. Компания HP не разглашает подробности своих политик безопасности, стремясь обеспечить целостность своих данных и систем. Тем не менее, ниже приводится краткое описание наших основных политик.

2. Организация информационной безопасности

   Компания HP разработала программу информационной безопасности, в рамках которой определена стратегия защиты информации в компании и реализуются меры по ее осуществлению. Эта система гарантирует, что в масштабах всей компании соблюдаются политики и меры безопасности, принятые в HP, а также требования к безопасности, устанавливаемые клиентами HP. Структура данной программы отвечает действующим в отрасли стандартам, законам и нормативным актам в области кибербезопасности, и программа ежегодно пересматривается с целью ее адаптации к меняющемуся ландшафту угроз, с которыми сталкивается компания HP.

3. Управление рисками кибербезопасности

   В компании HP реализована программа управления рисками кибербезопасности, направленная на сохранение конфиденциальности, целостности и доступности информационных активов компании. Эта программа обеспечивает последовательный подход к выявлению, оценке, определению приоритетности, снижению и устранению рисков кибербезопасности, минимизации последствий от них, а также ведению соответствующей отчетности. Компания HP определяет приемлемый уровень риска (Risk Appetite) как допустимый уровень потерь, а устойчивость к риску (Risk Tolerance) — как степень отклонения от этого приемлемого уровня риска. Риски оцениваются по строго определенной методике, что позволяет компании HP снижать риски информационной безопасности до приемлемого уровня. Данная программа согласуется с процессом управления рисками предприятия, действующим в компании HP.

Последнее обновление: сентябрь 2024 г.

4. Безопасность в области управления персоналом

   Политика компании HP в сфере безопасности персонала обеспечивает защиту информации на протяжении всего периода взаимоотношений между сотрудником и компанией, устанавливая процедуры доступа к помещениям, информационным системам и другим активам. Сюда входят процедуры проверки биографических данных, а также получение письменных подтверждений посредством заключения соглашений о конфиденциальности и неразглашении. Все соискатели на трудоустройство в компании HP должны проходить проверку биографических данных в соответствии с действующими законами, нормативными актами и этическими нормами.

5. Управление активами

   В компании HP реализован процесс, в рамках которого выявляются технические информационные активы, классифицируются критически важные активы и соблюдаются документированные процедуры по обращению с информацией каждого классифицированного типа, включая активы, содержащие персональные данные. Эти процедуры охватывают хранение, передачу и обмен информацией, доступ к ней, ведение журналов, сроки хранения, уничтожение и утилизацию, урегулирование инцидентов и уведомление о нарушениях. Политики и стандарты безопасности компании HP также устанавливают требования к безопасной утилизации носителей.

6. Безопасность данных

   Принятая в компании HP программа по обеспечению безопасности данных определяет методики и технические средства, которые должны быть внедрены для сохранения конфиденциальности, подлинности и целостности данных. Действующая в HP политика обеспечения безопасности данных предусматривает классификацию информации в соответствии с такими факторами, как требования законодательства, ценность и значимость информации, а также серьезность последствий ее несанкционированного разглашения или изменения. В дополнение к процедурам по обращению с данными, эта политика также регламентирует шифрование, удаление, сбор и обработку данных, сроки хранения и резервное копирование данных, а также предотвращение потери данных.

7. Контроль доступа

   Компания HP использует принцип наименьших привилегий для логического контроля доступа. Доступ каждого пользователя осуществляется с использованием уникального идентификатора пользователя и пароля. Политика паролей определяет меры по обеспечению сложности, надежности и действительности паролей, а также отслеживанию истории их использования. Права доступа периодически пересматриваются и аннулируются в случае увольнения сотрудников из компании. В рамках тех или иных форм взаимодействия с клиентами для предоставления доступа к клиентским системам и аннулирования такого доступа применяются заранее согласованные процедуры создания и удаления учетных записей пользователей.

8. Шифрование

   В компании HP разработан ряд надежных процессов шифрования для сохранения конфиденциальности, целостности и доступности информационных активов. Применяются утвержденные протоколы, требующие шифрования определенных активов, включая активы, содержащие персональные данные. Наша программа шифрования предполагает применение математических методов для защиты информации и передаваемых данных, исключая возможность несанкционированного доступа к ним. Защита данных от несанкционированного доступа и изменения является важнейшим элементом программы информационной безопасности компании HP.

9. Физическая и инфраструктурная безопасность

   Для защиты зданий и сооружений компании HP используются различные физические и электронные средства контроля и управления доступом, включая охранный персонал, электронные средства контроля доступа и системы видеонаблюдения. Объекты также оснащаются необходимой инфраструктурой, в том числе системами контроля и регулирования температуры и резервными источниками электропитания с применением ИБП и (или) дизельных генераторов для поддержания работы критически важных служб. Все сотрудники HP зарегистрированы и обязаны носить соответствующие идентификационные бейджи.

10. Управление деятельностью

    В компании HP установлены минимальные требования к обеспечению защиты технологической инфраструктуры, включая рабочие станции, серверы и сетевое оборудование. На этих устройствах используются образы операционных систем с параметрами, настроенными для обеспечения более высокого уровня безопасности, при этом требования варьируются в зависимости от операционной системы и реализуемых мер. Кроме того, компания HP внедрила системы обнаружения и предотвращения сетевых вторжений (NIDS/NIPS), которые находятся под круглосуточным наблюдением и контролем.

11. Безопасность связи

    Безопасность связи обеспечивает защиту информации, передаваемой по корпоративным сетям. Сюда входят установка компонентов сетевой безопасности (например, брандмауэров) и управление ими, разделение сетей, а также средства веб-фильтрации и обработки электронной почты. Это также предусматривает мониторинг каналов связи и управление ими с целью выявления и предотвращения фактов несанкционированного доступа или утечки данных.

12. Безопасность систем

    Политика компании HP предписывает применять такие методы разработки, которые обеспечивают безопасность систем и программного обеспечения на протяжении всего их жизненного цикла. Жизненный цикл разработки программного обеспечения охватывает подготовку, разработку или приобретение, внедрение, эксплуатацию и утилизацию. Все компоненты системы оцениваются с точки зрения их влияния на общую безопасность. Компания HP разрабатывает и внедряет средства обеспечения безопасности транзакций в рамках приложений, которые включают валидацию

учетных данных пользователей, использование цифровых подписей, шифрование, применение протоколов безопасной связи и хранение данных о транзакциях в зоне сети с соответствующим уровнем безопасности. Также регулярно проводится проверка на наличие возможных внутренних уязвимостей.

13. Третьи стороны и субподрядчики

    В компании HP реализованы процессы, позволяющие отбирать подрядчиков, полностью удовлетворяющих требованиям к безопасности, которые устанавливаются в договорах. В отношении соответствующих поставщиков, которые работают с данными компании HP или ее клиентов либо имеют доступ к сети компании HP, служба кибербезопасности компании HP проводит оценку рисков с целью проверки программы информационной безопасности, включающей физические, технические и административные средства и меры защиты. Эта оценка должна быть проведена до того, как поставщик получит доступ к информации компании HP.

14. Урегулирование инцидентов информационной безопасности

    В компании HP реализован комплексный процесс управления киберинцидентами, который определяет цели, сферу применения, роли, обязанности рядовых сотрудников и руководства, координирование действий отдельных подразделений, процедуры внедрения и проверку соответствия требованиям. Этот процесс анализируется и обновляется на ежегодной основе. Группа реагирования на киберинциденты, в которую входят сотрудники службы кибербезопасности компании HP, прошедшие обучение в области реагирования на инциденты и управления кризисными ситуациями, регулярно анализирует данный процесс с применением элементов моделирования, равно как анализирует любые инциденты и события.

15. Обеспечение непрерывности деятельности

    В компании HP действует глобальная программа по обеспечению непрерывности деятельности, которая гарантирует непрерывность деятельности в масштабах всей компании за счет стандартизированных и документированных процессов совместного планирования. Компания периодически анализирует свои планы по обеспечению непрерывности деятельности на предмет их эффективности, проверяя и обновляя все планы не реже одного раза в год. Кроме того, весь персонал, участвующий в реализации плана по обеспечению непрерывности деятельности, проходит соответствующее обучение.

16. Соответствие требованиям

    Политика соответствия установленным требованиям определяет подход компании HP к соблюдению правовых, договорных и внутренних требований, предъявляемых к эффективной программе информационной безопасности. Регулярный анализ информационной безопасности гарантирует внедрение необходимых протоколов в деятельность каждой бизнес-группы. Кроме того, в процессе такого анализа в документацию вносятся поправки, отражающие актуальные требования законодательства с учетом их изменения.

17. Индустрия платежных карт

    Свод правил и принципов индустрии платежных карт определяет подход компании HP к соблюдению требований этой индустрии, помогая компании HP понять ее роль и ответственность, а также внедрять необходимые меры обеспечения безопасности в соответствии с требованиями стандартов безопасности данных, действующих в индустрии платежных карт. Компания HP добивается соответствия требованиям индустрии платежных карт за счет установки и поддержания работы средств сетевой безопасности, например брандмауэров.

18. Безопасность продукции компании HP

    Для обеспечения безопасности своей продукции компания HP использует такие основные методы, как защита программного кода цифровой подписью, управление уязвимостями в продукции, выпуск информационных бюллетеней по безопасности и информирование о проблемах с безопасностью продукции. Эти меры гарантируют безопасность продукции компании HP для пользователей и их надежность. Безопасность продукции имеет первостепенное значение для компании HP, поскольку она способствует сохранению доверия клиентов и защищает от возможных угроз.

19. Безопасность услуг компании HP

    Компания HP использует ряд базовых методов для обеспечения безопасности услуг и сервисов, которые она предоставляет своим клиентам. Данная политика охватывает различные среды, в которых требуется обеспечивать безопасность услуг, в том числе среды, размещенные в инфраструктуре, которая принадлежит компании HP, третьим лицам, партнерам, а также клиентам. Эти меры гарантируют безопасность услуг компании HP для пользователей и их надежность. Внедряя надежные методы защиты и обеспечения безопасности, компания HP гарантирует безопасность и целостность своей продукции и услуг, способствуя созданию безопасной и заслуживающей доверия среды для всех пользователей.