Инструкции по соблюдению Стандарта защиты данных (PA-DSS) в платежном приложении RES версии 4.3 Hotfix 1 или выше

Общая Информация

Об этом Документе

Этот документ представляет собой краткое руководство с инструкциями для клиентов, дилеров и специалистов по системной интеграции с целью приведения программного решения для ресторанов **RES** в соответствие с требованиями стандарта **PCI DSS.** Этот документ относится исключительно к указанным ниже версиям решения **MICROS Restaurant Enterprise Solution (RES).**

Š **RES 4.3 Hotfix 1** и выше

Выполнение определенных действий для защиты вашей системы необходимо для обеспечения соответствия требованиям индустрии платежных карт (PCI).

Декларации

Гарантии

Несмотря на то, что все усилия прилагаются к тому, чтобы обеспечить полноту и корректность содержащейся в этом документе информации, **MICROS Systems, Inc.** не дает каких бы то ни было гарантий в отношении этого материала, включая, но не ограничиваясь, подразумеваемыми гарантиями рыночной конкурентоспособности и пригодности для тех или иных целей.

Информация, содержащаяся в этом документе, может изменяться без предварительного уведомления.

Ни одна из частей этого документа не может быть переиздана или предана гласности ни в какой форме и никакими средствами, электронными или механическими, включая фокопирование, перезапись, сохранение в информационно-поисковую систему, для каких бы то ни было целей, за исключением целей личного использования, без предварительного письменного согласия **MICROS Systems, Inc.**

MICROS Systems, Inc. не несет ответственности за ошибки, которые могут содержаться в этом документе, а также за случайные или косвенные убытки, связанные с предоставлением или использованием этого материала.

Торговые марки

FrameMaker – это зарегистрированная торговая марка Adobe Corporation.

Microsoft, Microsoft Excel, Win32, Windows, Windows→95, Windows 2000 (Win2K) и Windows NT – это торговые марки или зарегистрированные торговые марки Microsoft Corporation в США и/или других странах.

Visio – это зарегистрированная торговая марка Visio Corporation.

Все другие торговые марки являются собственностью соответствующих владельцев.

О соответствии требованиям PCI

Когда клиенты расплачиваются с помощью банковской карточки в точках продаж или совершают покупки через интернет, по телефону или электронной почте, они хотят быть уверенными в безопасности своего банковского счета. Вот почему был введен стандарт защиты данных индустрии платежных карт **(PCI DSS).** Эта программа призвана защищить данные держателей карт —независимо от места нахождения этих данных— и обеспечить поддержание самого высокого уровня стандарта информационной безопасности со стороны членов-участников, торгово-сервисных предприятий и провайдеров услуг[1].

Более подробно о соответствии требованиям **PCI** читайте на вэб-сайте Совета по развитию стандартов безопасности данных индустрии платежных карт **PCI SSC,** https://www.pcisecuritystandards.org/.

О стандарте безопасности данных индустрии PCI

Соответствие стандарту **PCI** требуется со стороны всех торгово-сервисных предприятий и провайдеров услуг, которые хранят, обрабатывают или передают данные о держателях карт. Эта программа касается всех каналов оплат, включая розничную торговлю через торговые точки, заказы товаров по электронной почте/телефону и интернет-коммерцию. Чтобы соответствовать требованиям **PCI**, торгово-сервисные предприятия и провайдеры услуг должны соблюдать Стандарт **PCI-DSS**, определяющий единый подход к обеспечению безопасности конфиденциальных данных для всех платежных брендов карточного рынка. Этот стандарт представляет собой результат совместного сотрудничества индустрии **PCI** и и призван создать общие для индустрии требования безопасности, включающие требования **PCI.**

Взяв за основу Стандарт **PCI-DSS,** индустрия **PCI** разработала и предлагает инструменты и меры защиты против утечки информации и компрометации карт для всей своей индустрии.
Стандарт **PCI-DSS**, описанный ниже, включает двенадцать основных требований, которые детализируются дополнительными требованиями:

Стандарт Безопасности Данных Индустрии PCI[2]

Построение и обслуживание защищенной сети

- **Требование 1:** Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт
- **Требование 2:** Не использовать настройки системных паролей и других параметров безопасности данных, заданных производителем по умолчанию

1. Reprinted from “Cardholder Information Security Program”, <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>.
2. Reprinted from the ‘PCI DSS Requirements and Security Assessment Procedures, v1.2’ document, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

Защита данных о держателях карт

- **Требование 3:** Обеспечить безопасное хранение данных о держателях карт
- **Требование 4:** Обеспечить шифрование данных о держателях карт при их передаче через открытые сети общего пользования

Программа управления уязвимостями

- **Требование 5:** Использовать и регулярно обновлять антивирусные программы
- **Требование 6:** Разрабатывать и поддерживать системы и приложения безопасности

Внедрение строгих мер контроля доступа

- **Требование 7:** Ограничить доступ к данным о держателях карт служебной необходимостью
- **Требование 8:** Привязать уникальный идентификатор всем, у кого есть доступ к ПК
- **Требование 9:** Ограничить физический доступ к данным о держателях карт

Регулярный мониторинг и тестирование сети

- **Требование 10:** Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт
- **Требование 11:** Регулярно тестировать системы и процессы информационной безопасности

Поддержание политики информационной безопасности

- **Требование 12:** Поддерживать политику информационной безопасности

Соблюдение требований PCI и Windows NT

Несмотря на то, что платформа **Windows NT** поддерживается продуктом **RES**, эта платформа не соответствует стандарту **PA-DSS** и не может использоваться там, где соблюдается стандарт **PA-DSS.**

Для кого предназначен этот документ

Этот документ предназначен для следующей аудитории:

- Установщики/Программисты **MICROS**
- Дилеры **MICROS**
- Служба ПоддержкиКлиентов **MICROS**
- Обучающий персонал **MICROS**
- Персонал **MIS**
- Клиенты **MICROS**

Необходимые предварительные знания

Этот документ рассчитан на аудиторию, имеющую следующие знания или навыки:

- Умение работать с ПК
- Понимание базовых сетевых концепций
- Опыт работы с **Windows 2000**, **Microsoft Windows XP Pro** или **Windows 2003**
- Знакомство с ПО **MICROS RES**
- Опыт работы с периферийными устройствами **MICROS**

RES и Стандарт Защиты Данных Индустрии PCI

Стандарт защиты данных индустрии PCI

В то время как **MICROS Systems Inc.** признает важность поддержания безопасности и целостности данных о держателях платежных карт, некоторые параметры Стандарта **PCI-DSS** и того, что касается соблюдения требований **PCI**, остается исключительной ответственностью клиента. Настоящий раздел содержит описание **12** пунктов Стандарта **PCI-DSS.** Информация в этом разделе касается только соответствия версии **1.0 RES** Стандарту **PCI-DSS.**

Поскольку платежное приложение должно работать в условиях защищенной сети, **RES** не препятствует использованию **NAT, PAT,** сетевого устройства фильтрации трафика, анти-вирусной защиты, установке патчей и обновлений, а также шифрованию.

Построение Документа

Этот документ по отдельности освещает каждое из **12** основных требований, изложенных в Стандарте **PCI DSS.** По каждому требованию приводится комментарий Группы Разработчиков **MICROS** или рекомендация, касающаяся программы **RES**.

Построение и Обслуживание Защищенной Сети

1. Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт

Межсетевые экраны - это средства вычислительной техники, контролирующие разрешенный входящий сетевой трафик, а также трафик между сегментами локальной сети разного уровня критичности. Все системы должны быть защищены от неавторизованного доступа через интернет, будь то электронная коммерция, удаленный доступ своих работников через браузер или корпоративная почта. Часто кажущиеся малозначимыми каналы связи с внешней средой могут представлять собой незащищенные пути доступа к ключевым системам. Межсетевые экраны – это основные механизмы обеспечения безопасности любой компьютерной сети.[3]

В соответствии со Стандартом **PCI DSS, MICROS Systems Inc.** настаивает на том, чтобы все объекты, включая тех, что работают с беспроводными сетями, установили и поддерживали межсетевые экраны для защиты данных. Сконфигурите вашу сеть так, чтобы базы данных и беспроводные точки доступа *всегда* располагались за межсетевыми экранами и не имели прямого доступа к Интернету.

3. “Payment Card Industry (PCI) Data Security Standard.doc”, p. 4, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Персональный защитный экран в виде ПО должен быть установлен на всех переносных и персональных компьютерах работников, где есть прямой выход в интернет, например, на ноутбуках, используемых работниками для доступа к сети организации. Работники не должны иметь возможности изменять конфигурационные настройки защитного экрана.

С целью обеспечить соблюдение Стандарта **PCI DSS**, **MICROS Systems Inc.** настаивает на том, чтобы серверы, базы данных, беспроводные точки доступа и любые среды с конфиденциальными данными на всех объектах находились за межсетевыми экранами. Конфигурация межсетевого экрана должна ограничивать соединения между серверами общего пользования и любыми системными компонентами, хранящими данные о держателях карт, включая любые беспроводные соединения.

Конфигурация межсетевого экрана должна учитывать размещение базы данных во внутренней сети, отделенной от демилитаризованной зоны **(DMZ)** вэб-сервером. Демилитаризованная зона может использоваться для отделения Интернета от систем хранения данных о держателях карт.

MICROS Systems, Inc. не рекомендует устанавливать межсетевой экран поставщика. Проработайте этот вопрос с сетевым администратором клиента и настройте то, что подходит для их конфигурации. **MICROS Systems, Inc.** имеет в продаже межсетевой экран, который может использоваться на объектах с программой **MICROS RES.** Более подробно о межсетевых экранах, предлагаемых **MICROS**, читайте **PMA05-828.**

Windows XP Pro, 2003 и **Vista** имеют встрроенный в программу межсетевой экран, который самостоятельно включается при запуске **MICROS RES.** Межсетевой экран должен быть активирован до установки программы **MICROS RES.**

Чтобы убедиться в том, что конфигурация межсетевого экрана соответствует Требованию **1** Стандарта **PCI DSS «**Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт**»**, читайте вэб-сайт Совета **PCI-SSC** https://www.pcisecuritystandards.org/

2. Не использовать настройки системных паролей и других параметров безопасности данных, заданных производителем по умолчанию

Хакеры (как на стороне, так и внутри компании) для взлома систем часто прибегают к использованию паролей и других настроек , заданных производителями по умолчанию. Эти пароли и настройки хорошо известны в определенных сообществах и легко находятся через открытые источники информации.[4]

RES позволяет менять пароли во всех приложениях, ОС и базах данных.

4. "Payment Card Industry (PCI) Data Security Standard.doc", p. 5, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Комплексными по умолчанию должны быть все пароли для всех администраторов и работников, имеющих доступ к администрированию.

MICROS не вправе за вас менять пароли. В Приложении **A** к этому документу содержится образец регистрационного журнала для всех смен паролей. См. раздел, начиная со стр. **27**.

Чтобы обеспечить соответствие требованиям PCI, дефолтовые настройки НЕОБХОДИМО изменить до запуска живого запуска системы на объекте. Все пароли должны меняться не реже, чем каждые 90 дней.

MICROS Systems, Inc. не рекомендует использовать учетные записи администратора, типа **"sa"**, для доступа к базе данных и входа в приложение. Клиентам и дилерам/специалистам по системной интеграции рекомендуется всегда привязывать надежные пароли к подобным дефолтовым учетным записям, даже если эти учетные записи не используются. Позднее, эти дефолтовые учетные записи должны быть отключены или перестать использоваться.

Когда в службу поддержки - вашу или третьего поставщика - поступает запрос на поддержку, то для оказания помощи может понадобиться один или несколько паролей. Всякий раз, когда пароль передается на сторону, он должен затем быть сменен, чтобы обеспечить соответствие требованиям **PCI**.

Помимо этого, **RES** имеет возможность навязывать комплексные пароли для входа во все приложения **Back Office**, включая модули программирования, отчетности и утилиты **Back Office**. Можно установить специальные требования к комплексным паролям, например, минимальную длину, буквенно-цифровой ввод, периодическую ротацию и блокировку после неуспешных попыток входа. **MICROS** рекомендует клиентам, использующим **RES**, устанавливать комплексные пароли для доступа к приложениям **Back Office**, в соответствии с **PA-DSS**.

Для всех системных компонентов, включая ОС, сетевые устройства и точки доступа, **MICROS** рекомендует изменять все дефолтовые пароли производителей на комплексные пароли.

Клиентам и дилерам/специалистам по системной интеграции рекомендуется контролировать доступ, используя уникальное имя пользователя и соответствующие стандарту **PCI DSS** комплексные пароли, ко всем ПК, серверам и базам данных с платежными приложениями и данными о держателях платежных карт.

Комплексная безопасность в RES

Надежные системные пароли и пароли для входа в приложение должны использоваться везде, где только возможно. **MICROS Systems, Inc.** настаивает на том, чтобы клиенты и дилеры/специалисты по системной интеграции всегда создавали комплексные пароли, соответствующие требованиям **PCI DSS**, для входа в платежные приложения.

Выполните следующие шаги для обеспечения комплексной безопасности в **RES:**

1. **О**ткройте *POS Configurator* | *System* | *Restaurant* | *Security* и отключите опцию **Use Classic Security**.

2. **С**конфигурите комплексные настройки защиты в соответствии с правилами для торгово-сервисных предприятий. Торгово-сервисное предприятие должно выполнять требования **PCI** и соответствовать Стандарту.

   В таблице ниже приведены возможные опции и минимальные рекомендуемые настройки. Все опции находятся в *POS Configurator* | *System* | *Restaurant* | *Security*.

Опция	Рекомендуемая настройка
Use Micros Classic Security	Всегда отключена.
Days Until Password Expires	**90** дней
Minimum Password Length	**7 с**имволов. Пароль должен содержать как цифры, так и буквы.
Maximum Idle Time in Minutes	**15** минут
Maximum Failed Logins	**6** попыток
Require AlphaNumeric Passwords	Всегда включена
Password Repeat Interval	**4**

Учетные записи пользователей Базы Данных RES

Для запуска **RES** необходимы две учетных записи пользователей базы данных: учетная запись администратора БД, и учетная запись пользователя **Micros**. Пароли для этих двух учетных записей базы данных необходимо изменить при вводе системы в эксплуатацию и в будущем продолжать менять их каждые **90** дней, для обеспечения соответствия требованиям **PCI**.

Поддержка Стороннего Приложения

Система **RES** допускает интеграцию с третьими производителями. Торгово-сервисное предприятие несет ответственность за осуществление интеграции с системой **RES.** В случае если производителю нужен доступ к базе данных или приложению **RES,** торгово-сервисное предприятие несет ответственность за предоставление и смену паролей. Если используется поддержка третьей стороны, **MICROS** рекомендует следующее:

- Создайте отдельные учетные записи пользователей базы данных для каждого производителя и ограничьте их права доступа необходимыми им функциями.
- Создайте отдельные учетные записи пользователей приложения **RES** для каждого производителя и ограничьте их права доступа необходимыми им функциями.
- Пароли администратора базы данных **RES** и пользователя **MICROS** нельзя раздавать. Если они передаются для оказания поддержки, их следует сменить немедленно после использования.

Беспроводные Среды

При использовании беспроводных сред измените дефолтовые настройки производителей, включая, но не ограничиваясь, следующим: ключи к беспроводным протоколам защиты данных **(WEP),** дефолтовый идентификатор беспроводной сети **(SSID),** дефолтовые пароли и строки имени и пароля **SNMP.** Отключите **SSID broadcasts** и включите технологию **Wi-Fi** защищенного доступа **(WPA2)** для шифрования и аутентификации. **Это необходимо сделать, чтобы соответствовать требованиям PCI.**

Более подробно смотрите документ «*MICROS Wireless Networking Best Practices: A Payment Application Data Security Standard (PA-DSS) Implementation Guide Supplement*».

Все вне-консольные входы под администратором должны шифроваться с использованием технологий **SSH, VPN** или **SSL/RLS (**протокол **TLS),** независимо от целей: будь то управление через интернет или другое. Ни **Telnet,** ни **rlogin** никогда не должны использоваться для администрирования.

Более подробно о Требовании **2** Стандарта **PCI DSS «**Не использовать настройки системных паролей и других параметров безопасности данных, заданных производителем по умолчанию**»,** читайте вэб-сайт Совета **PCI-SSC** https://www.pcisecuritystandards.org/

Защита данных о держателях карт

3. Защита данных о держателях карт

Шифрование – это лучший механизм защиты, потому что даже если кто-то взломает все другие механизмы защиты и получит доступ к зашифрованным данным, он не сможет их прочитать, не имея ключа шифрования. Шифрование - пример принципа многоуровневой защиты.[5]

MICROS следующим образом интерпретирует это требование:

1. **Не храните полные данные дорожек после авторизации.**

   Ни при каких условиях **RES** не будет сохранять полные данные дорожек.

2. **Не разрешать доступ к полным номерам кредитных карт в торговой точке. Также, прятать или шифровать номера кредитных карт при их распечатке или хранении.**

   С появлением **RES**, существующие опции, позволяющие скрывать данные, продолжают использоваться. Что касается номера кредитной карты **(PAN)**, то система прячет все, за исключением последних четырех цифр. Дата окончания срока действия полностью скрывается, а имя держателя карты не печатается. Сокрытие данные происходит всякий раз при печати или отображении данных на дисплее, когда есть риск доступа постороннего к этим данным. То же касается и дисплеев рабочих стаций, периферийных устройств **(**дисплеев на шесте, наладонников, коммутационных панелей**)**, а также системных отчетов, журналов и логов.

   Следующие опции ДОЛЖНЫ быть настроены до живого запуска системы, с целью обеспечить соответствие требованиям PCI:

   - **POS Configurator | Sales | Tender/Media | CC Tender | Mask Credit Card Number. О**пция должна быть включена.
   - **POS Configurator | Sales | Tender/Media | CC Tender | Mask Expiration Date. О**пция должна быть включена.
   - **POS Configurator | Sales | Tender/Media | CC Tender | Mask Cardholder Name. О**пция должна быть включена. Когда эта опция включена, имя держателя карты не сохраняется в базе данных.

Все данные авторизации кредитных карт, сохраняющиеся в системе **RES**, шифруются и регулярно удаляются. Удаление данных кредитных карт должно быть настроено в соответствии с рекомендациями вашего процессингового банка. Данные о держателях карт, срок хранения которых превысил период, устанавливаемый торгово-сервисным предприятием, должны стираться.

5. "Payment Card Industry (PCI) Data Security Standard.doc", p. 6, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Чтобы сконфигурить очистку данных кредитных карт, зайдите в ***POS Configurator | System |Restaurant | Business Settings*** и введите значение в поле ***Save Batch Records | Number of Day***. Этим значением должно быть **15 дней**.

Надежное удаление архивных данных

Архивные данные (данные магнитной полосы, валидационные коды карт, **PIN**-номера или **PIN**-блоки), которые сохранялись предыдущими версиями ПО **MICROS**, необходимо надежно удалить, чтобы соблюсти требования **PCI**. См. документ ***RES Upgrade Best Practices***, содержащий инструкции, описывающие удаление таких данных.

Когда делается обновление с более ранней версии **MICROS RES** (версия **3.2 SP 7 HF 4** или ниже), то при конверсии архивные данные сохраняются в базе данных.

Обновления с версий, не соответствующих требованиям **PCI**, до версии, соблюдающей эти требования, должны включать форматирование всех системных жестких дисков и установку на них ПО. Как альтернативный вариант, можно надежно стереть все старые базы данных, лог-файлы и все другие файлы, содержащие конфиденциальные данные.

Все криптографические данные, например, ключи шифрования, верификации данных о держателях карт или конфиденциальные данные аутентификации, хранившиеся предыдущими версиями ПО, должны быть надежно удалены, чтобы обеспечить соответствие требованиям **PCI**. См. документ ***RES Upgrade Best Practices***, ***MD0003-135***, содержащий инструкции, описывающие надежное удаление этих данных.

Сбор конфиденциальных данных аутентификации для диагностики и решения проблем

Иногда дилерам/специалистам по системной интеграции **MICROS RES** приходится диагностировать и устранять проблемы в системе.

В целях обеспечения защиты данных о держателях карт, **MICROS Systems, Inc.** настаивает на том, чтобы дилеры/ специалисты по системной интеграции **MICROS RES** собирали только те конфиденциальные аутентичные данные (например, конфиденциальные данные аутентификации, лог-файлы, отладочные файлы, базы данных и т.п.), которые действительно необходимы для решения конкретной проблемы. Такие данные необходимо хранить только в специальном, знакомом месте с ограниченным доступом.

Дилеры/ специалисты по системной интеграции должны собирать только ограниченный объем данных, действительно необходимый для решения конкретной проблемы, и при хранении шифровать такие конфиденциальные данные аутентификации. Когда данные больше не нужны, их необходимо сразу же и надежно удалить.

При диагностике и устранении софтверных проблем, дилеры и специалисты по системной интеграции, работая с базами данных действующих объектов, должны помнить о следующем:

- Š Запрашивать живые базы данных действующих клиентов следует, только когда необходимо решить конкретную проблему. Если база данных необходима для оказания поддержки, ее следует разместить на **FTP** сайте клиентской поддержки **MICROS.** Читайте документ ***MICROS FTP Site File Transfer Policy***.

- Š Хранить базы данных в специальных, знакомых местах с ограниченным доступом. Защищать паролем **zip а**рхивы, используемые для хранения баз данных клиентов.

- Š Запрашивать только ограниченный объем данных, необходимый для решения конкретной проблемы. Размещать самый последний бэкап базы данных, а не все бэкапы, в директории **\DbBackups**. Чем больше у вас файлов, тем больше информации вам придется контролировать, и тем больше файлов вам придется удалить позднее. Об удалении файлов, читайте документ **MICROS *Secure Wipe Tool*.**

- Š Надежно удалять такие данные немедленно по окончании их использования. Речь идет об удалении данных с того ПК или терминала, на котором устранялась проблема.

Прим*: При использовании драйвера CAPMS с RES, опция Devices | Interfaces | Log Transactions должна быть включена только на период устранения проблемы. Эта опция должна быть всегда отключена при выполнении CAPMS транзакций, не связанных с устранением проблем.*

Более подробно читайте документ *Customer Support Information Security Guidelines,* который можно найти в разделе *Member Services* на вэб-сайте **MICROS** (*www.members.micros.com*).

Шифрование данных

Конфиденциальные данные кредитных карт **(**номер персонального счета, дата окончания срока действия, имя клиента**)** шифруются в системе **RES** на время их хранения. **RES** надежно шифрует данные, используя промышленный стандарт алгоритмов **- 3DES** и **AES.**

RES хранит информацию в трех местах:

- Š в локальной базе данных торговой точки,

- Š в резервной базе данных на сервере, и

- Š в базе данных **SAR** клиента **(**удаленно**).**

В каждом из этих мест хранится и конфиденциальная, и не конфиденциальная информация. На сервере сохраняются все три копии, но только две последние есть локально на каждом клиенте.

Что касается локальной базы данных в торговой точке, то **RES 4.0** шифрует ее полностью, используя стандартное **AES** шифрование. Эта процедура не конфликтует с приложениями, работающими в системе **RES** и имеющими доступ к базе данных через стандартные инструменты **SQL**. Шифрование файла базы данных предотвращает неавторизованный доступ через бинарные редакторы и/или гексагональные утилиты содержимого памяти.

Помимо первичного шифрования базы данных, второй уровень шифрования применяется к конфиденциальным данным, перед тем как они помещаются на хранение в базу данных. Это делается на уровне приложения программой, которая записывает данные в базу данных. Когда это необходимо, только отдельные приложения будут шифровать данные. Для всех других пользователей, эти данные будут отображаться в закодированном виде при попытке открыть их через инструменты **SQL**.

Парадигма безопасности **RES** требует использовать ключи шифрования для :

- шифрования базы данных.
- шифрования конфиденциальных полей в базе данных.
- шифрования конфиденциальных данных, передаваемых по сети.

RES позволяет конечному пользователю в любое время менять фразы-пароли для этих ключей. Это относится к понятию ротации ключей. Во время ротации ключей базы данных, вся база данных должна быть выгружена и снова загружена, а все архивные данные – повторно зашифрованы. На эту работу может уйти часов семь, в зависимости от размера базы данных. Во время ротации ключей конфиденциальных данных, система будет выключена, а все архивные данные будут повторно зашифрованы с помощью нового ключа.

Эти фразы-пароли ДОЛЖНЫ быть изменены до живого запуска системы и затем меняться, по меньшей мере, раз в год – с целью соответствия требованиям PCI

Для смены фраз-паролей используйте **RES Database Manager**. Пользователям не нужно вводить фразу-пароль. **RES Database Manager** автоматически сам выберет фразу-пароль - буквенно-цифровую.

RES также шифрует транспортировку конфиденциальных данных между **POS** клиентом и **RES** сервером. Для этого транспортного шифрования используется шифрование **RES**. Пара ключей - секретный и открытый - находится на сервере **RES** и сервере бэкапа. У каждого **POS** клиента есть только открытый ключ.

MICROS рекомендует менять транспортный ключ шифрования раз в год, по меньшей мере.

Используйте **RES Database Manager** для смены фраз-паролей и транспортного ключа шифрования.

Выполните следующие шаги для смены ключа шифрования/фразы-пароля к базе данных или данным:

1. Откройте RES Database Manager
2. Откройте закладку *Encryption key*
3. Выберите опцию **Change Database** и/или **Change Data Key**.
4. Нажмите кнопку **CHANGE ENCRYPTION KEY**. Система автоматически выберет новую буквенно-цифровую фразу-пароль.

Выполните следующие шаги для смены Транспортного Ключа Шифрования:

1. Откройте RES Database Manager.
2. Откройте закладку *Encryption key*.
3. Выберите опцию **Change Transport Key**.
4. Нажмите кнопку **CHANGE ENCRYPTION KEY**.

Более подробно о Требовании **3** Стандарта **PCI** "Защита данных о держателях карт", читайте вэб-сайт Совета **PCI-SSC** https://www.pcisecuritystandards.org/

4. Обеспечить шифрование данных о держателях карт при их передаче через открытые сети общего пользования

Конфиденциальная информация, при передаче ее через интернет, должна зашифровываться, так как хакеру легко и просто перехватить и/или перенаправить такие данные.[6]

При передаче данных о держателях карт через сети общего пользования или интернет всегда используйте протокол **SSL** версии **3.0**, а при беспроводной передаче - всегда используйте самый высокий доступный уровень шифрования. Более подробно читайте *MICROS Wireless Networking Best Practices: A Payment Application Data Security Standard (PA-DSS) Implementation Guide Supplement.*

В целях соответствия стандарту **PCI DSS, MICROS Systems Inc.** настаивает на использовании надежной технологии шифрования при передачи данных (например, **IPSEC, VPN** или **SSL/TLS**), при отправке информации о держателях карт через сети общего пользования, в т.ч. при использовании беспроводных соединений, **E-mail** и сервисов типа **Telnet, FTP** и пр. При отправке номеров кредитных карт по **E-mail,** клиенты и дилеры должны использовать решение для шифрования электронной почты.

6. "Payment Card Industry (PCI) Data Security Standard.doc", p. 7, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Модемы не должны располагаться на серверах приложений, за исключением безвыходных ситуаций. Если модем установлен, он должен быть отключен от питания или выключен все то время, пока не используется. Для большей безопасности модем должен быть сконфигурен для автоматического возврата вызова и шифрования данных. Межсетевые экраны не защитят против атак через модем.

Любой вне-консольный вход под администратором, для управления через интернет или других целей, должен быть зашифрован с использованием технологий типа **SSH, VPN** или **SSL/RLS (**протокол **TLS).** **Telnet** или **rlogin** никогда не должны использоваться для администрирования.

Конфиденциальные данные, передаваемые между **POS** клиентом и сервером, шифруются с помощью **RSA (**а-симметричный механизм шифрования**)** в проводных и беспроводных сетях. Помимо этого, **RES** поддерживает шифрование на уровне протокола операционной системы и сетевого оборудования, как например, протокол **WEP, IPSEC** и **WPA.**

Беспроводная передача данных о держателях кредитных карт должна шифроваться как в сетях общего пользования, так и в частных сетях. Шифруйте передачу данных, используя технологию **WPA** или **WPA2,** протоколы **IPSEC VPN** или **SSL/TLS.** Никогда не доверяйтесь исключительно протоколу **WEP** для защиты конфиденциальности и входа в беспроводную сеть **LAN.**

Используйте один из вышеупомянутых способов в сочетании с **128-**битным протоколом **WEP** и ежеквартально делайте ротацию ключей общего пользования для **WEP (**или автоматически, если позволяет технология**),** а также всегда, когда делаются перестановки в кадрах, имеющих доступ к ключам. Для протокола **WEP** необходимо использовать, по меньшей мере, **104-**битный ключ шифрования и **24-**битное значение инициализации. Всегда ограничивайте доступ на базе **MAC** адреса.

Конфиденциальные данные, хранимые в базе данных **MICROS,** шифруются с помощью надежного алгоритма шифрования **(Triple-DES).** Конфиденциальные данные - это номер счета держателя карты, дата окончания срока действия, имя держателя карты, а также пароли входа в приложение. Ротацию ключа шифрования может делать конечный пользователь.

Файл с базой данных **MICROS** шифруется с помощью **AES.** Фраза-пароль для базы данных **MICROS** может меняться конечным пользователем.

Более подробно о Требовании **4** Стандарта **PCI DSS, "**Обеспечить шифрование данных о держателях карт при их передаче через открытые сети общего пользования**",** читайте вэб-сайт Совета **PCI SSC** https://www.pcisecuritystandards.org/

Программа Управления Уязвимостями

5. Использовать и регулярно обновлять антивирусные программы

Много уязвимостей и вредоносных вирусов попадает в сеть через электронную почту. Чтобы защититься от них, антивирусные программы должны быть установлены на всех почтовых системах и рабочих столах.[7]

В соответствии со стандартом **PCI DSS, MICROS Systems Inc.** настаивает на регулярном использовании и обновлении антивирусного ПО**. MICROS** регулярно тестирует новые релизы антивирусных программ**,** выпускаемые **Norton®** и **McAfee®,** а также обновления безопасности от **Microsoft®,** и предоставляет ежемесячные отчеты о результатах тестов дистрибуторам**.** Валидация большинства обновлений занимает **1** неделю и дальше меньше в случае критических обновлений**.**

Антивирусное ПО должно быть размещено на всех системах**,** обычно подверженных заражению вирусами**,** в особенности на всех ПК и серверах**.**

Чтобы убедиться в том**,** что ваша анти**-**вирусная программа настроена в соответствии с Требованием **5** Стандарта **PCI DSS, "**Использовать и регулярно обновлять антивирусные программы**",** читайте вэб**-**сайт Совета **PCI SSC** https://www.pcisecuritystandards.org/

6. Разрабатывать и поддерживать системы и приложения безопасности

Злоумышленники используют уязвимости в защите для проникновения в системы. Многие из этих уязвимостей устраняются обновлениями безопасности, выпускаемыми производителем, поэтому все системы должны обновляться актуальными программными патчами, защищающими от злоумышленных действий работников, сторонних хакеров и вирусов. Что касается приложений, являющихся продуктом собственных рабработок, то здесь многочисленных уязвимостей можно избежать, используя стандартные процессы разработки систем и защитное кодирование.[8]

MICROS Systems Inc. использует стандартные процедуры развития системы для обеспечения программной целостности и безопасности**,** включая использование отдельных сред для разработок**/**тестирования и производства**,** и разграничение функциональных обязанностей между этими средами**.** Обновленные сервис**-**паки и хот**-**фиксы доступны на вэб**-**сайте **MICROS** <http://www.micros.com>.

7. "Payment Card Industry (PCI) Data Security Standard.doc", p. 8, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.
8. "Payment Card Industry (PCI) Data Security Standard.doc", p. 8, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

В то время как **MICROS** прилагает все возможные усилия к тому, чтобы соответствовать Шагу **6** Стандарта **PCI-DSS**, некоторые параметры, в т.ч. процедуры изменений конфигураций систем и программ, а также установка доступных обновлений безопасности, зависят от специфической практики и политики объекта.

Для соответствия Требованию **6** Стандарта **PCI DSS**, необходимо регулярно обновлять все операционные системы **(**ОС**)** и устанавливать на них патчи. Когда выпускаются критические обновления, их необходимо устанавливать, чтобы поддерживать безопасность системы на максимально высоком уровне. На всех ПК также должны быть установлены анти-вирусные определения, которые надо регулярно обновлять свежими определениями вирусов. Проверяйте документацию, предоставляемую вашим провайдером анти-вирусных программ, а также ту, что касается вашей ОС, на наличие у вас всех последних обновлений.

Для обеспечения соответствия требованиям **PCI**, необходимо отключить и сохранять отключенной опцию *Восстановления Системы* **Microsoft Windows XP Pro.** Чтобы отключить Восстановление Системы, выполните нижеуказанные шаги:

1. Откройте *Start Menu* go to the *My Computer* | *Properties* | *System Properties* | *System Restore* и включите либо опцию **Turn off System Restore**, либо опцию **Turn off System Restore on all drives**.
2. Нажмите **[Ok]**.
3. Когда появится нижеуказанное сообщение, нажмите **[Yes]** для подтверждения того, что вы хотите отключить Восстановление Системы:

   ```
   Вы выбрали отключение Восставления Системы. Если вы
   подтвердите, все существующие точки восстановления будут
   удалены, и вы не сможете отследить или отменить
   изменения на вашем компьютере.
   Хотите отключить Восстановление Системы?
   ```

4. Диалоговое окно *System Properties* закроется. Выполните шаги, чтобы включить Восстановление Системы.

Выполните эти шаги для включения Восстановления Системы:

1. Откройте *Start Menu* go to the *My Computer* | *Properties* | *System Properties* | *System Restore*.
2. **С**отрите опцию **Turn off System Restore** или опцию **Turn off System Restore on all drives**.
3. Нажмите **[Ok]**.
4. Диалоговое окно *System Properties* закроется.

Чтобы убедиться в том, что ваш сайт разрабатывает и поддерживает системы и приложения безопасности в соответствии с Требованием **6** Стандарта **PCI DSS, "**Разрабатывать и поддерживать системы и приложения безопасности**",** читайте вэб-сайт Совета **PCI SSC** https://www.pcisecuritystandards.org/

Внедрение строгих мер контроля доступа

7. Ограничить доступ к данным служебной необходимостью

Доступ к критическим данным предоставляется только авторизованным пользователям.[9]

MICROS признает важность контроля доступа к данным и осуществляет этот контроль, предоставляя доступ в зависимости от уровня должности работника. Этот механизм позволяет ограничить доступ к конфиденциальной информации необходимым для выполнения должностных обязанностей объемом информации и защитить пароли.

Доступ к паролям клиентов со стороны дилеров и специалистов по системной интеграции должен быть ограничен.

Более подробно о Требовании **7** Стандарта **PCI DSS, "**Ограничить доступ к данным служебной необходимостью**",** читайте на вэб-сайте Совета PCI SSC https://www.pcisecuritystandards.org/

8. Привязать уникальный идентификатор каждому, у кого есть доступ к ПК

Такая привязка гарантирует, что действия с критическими данными и системами выполняются известными и авторизованными пользователями и могут отслеживаться.[10]

MICROS Systems Inc. признает важность привязки уникального идентификатора каждому работнику, имеющему доступ к компьютеру. Два разных пользователя **MICROS** не могут иметь одинаковый идентификатор, что позволяет отслеживать действия каждого при условии, что клиент поддерживает должную конфигурацию и ограничивает уровни привилегий работников служебной необходимостью.

В то время как **MICROS** прилагает все возможные усилия к тому, чтобы соответствовать Шагу **8** Стандарта **PCI-DSS,** некоторые параметры, в т.ч. аутентификация пользователя, удаленный доступ к сети и управление паролями для производственно-технического персонала и администраторов, а также для всех системных компонентов, зависят от специфической практики и политики того или иного объекта.

9. "Payment Card Industry (PCI) Data Security Standard.doc", p. 9, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.
10. "Payment Card Industry (PCI) Data Security Standard.doc", p. 10, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Все торгово-сервисные предприятия ДОЛЖНЫ распространить эти инструкции среди всех пользователей системы, чобы обеспечить соответствие требованиям **PCI**.

Создание Надежных Паролей

Для обеспечения соответствия Требованию **8** Стандарта **PCI DSS, RES** позволяет клиентам настаивать на установке комплексных паролей для доступа к функциям администрирования и **Back-of-House**. Логика комплексных паролей подразумевает ввод правильного имени пользователя и пароля для входа во все приложения. Имя пользователя должно быть уникальным.
Для установки комплексных паролей в **POS** Конфигураторе в форме *System* | *Restaurant* | *Security* предусмотрены следующие опции:

- **Days Until Expiration**
  Введите количество дней, в течение которых пароль может оставаться активным, прежде чем его необходимо сменить.
  Необходимая настройка: не более **90**

- **Minimum Password Length**
  Введите необходимое минимальное количество символов для длины пароля.
  Необходимая настройка: по меньшей мере, **7**

- **Password Repeat Interval**
  Введите количество разных паролей, которые должны попеременно использоваться, прежде чем можно будет повторить старый пароль.
  Необходимая настройка: по меньшей мере, **4**

- **Require Alphanumeric Passwords**
  Выберите эту опцию, чтобы пароль был буквенно-цифровым.
  Необходимая настройка: поставить галочку **(**включено**)**

- **Maximum Allowed Failed Logins**
  Введите допустимое количество неудачных попыток входа, прежде чем учетная запись пользователя будет заблокирована.
  Необходимая настройка: не более **6**

- **Maximum Idle Time**
  Введите количество минут, в течение которых административное приложение может оставаться в бездействии, прежде чем все несохраненные изменения будут удалены, и приложение отключится, после чего пользователю придется снова выполнять процедуру входа.
  Необходимая настройка: не более **15** минут

Для обеспечения строгого контроля доступа к приложению **RES,** всегда привязывайте уникальные имена пользователей и комплексные пароли к каждой учетной записи. **MICROS Systems Inc.** настаивает на применении этих инструкций не только к паролям **MICROS,** но и к паролям **Windows**®.

Более того, **MICROS Systems, Inc.** советует пользователям, посредством уникального имени пользователя и комплексного пароля, соответствующих требованиям **PCI**, контролировать доступ ко всем ПК, серверам и базам данных с платежными приложениями и данными о держателях кредитных карт.

Удаленный Доступ

MICROS Systems, Inc. настаивает на использовании двух-факторной аутентификации для предоставления удаленного доступа к сети объекта со стороны работников **MICROS Systems, Inc.**, администраторов и представителей третьих сторон. Необходимо использовать такие технологии, как Служба удаленной аутентификации пользователей по телефонным линиям **(RADIUS)**, Система управления доступом для контроллера доступа к терминалу **(TACACS)** с токенами, или **VPN** на базе протоколов **SSL/TLS** или **IPSEC** с отдельными сертификатами.

Функциональность защиты удаленного доступа к программному обеспечению всегда должна быть установлена и использоваться. Дефолтовые настройки для удаленного доступа к программному обеспечению необходимо менять, с тем чтобы у каждого клиента были свои уникальные имя пользователя и комплексный пароль.

Никогда не используйте дефолтовый пароль, и когда создаете новый, надежный пароль для удаленного доступа к программному обеспечению, соблюдайте Требование **8** Стандарта **PCI DSS (**см. стр. **21)**. Никогда не используйте дефолтовый пароль и соблюдайте требования Стандарта **PCI DSS** при создании паролей для клиентов. Пароли должны содержать, по меньшей мере, **8 с**имволов и быть буквенно-цифровыми.

Подключения должны разрешаться только со специальных, известных **IP/MAC а**дресов. Для входа необходимо использовать надежную аутентификацию или комплексные пароли. Необходимо, чтобы была включена опция блокировки передачи зашифрованных данных и учетной записи после определенного количества неуспешных попыток. Система должна быть сконфигурена таким образом, чтобы удаленному пользователю для получения доступа приходилось устанавливать **VPN** соединение через межсетевой экран.

В целях защиты данных, необходимо включить функциональность входа через идентификатор пользователя. Отключать эту функциональность не следует, так как это противоречит требованиям **PCI DSS**. Доступ к паролям клиентов должен иметь только персонал авторизованных дилеров/ специалистов по системной интеграции. Более подробно, читайте документ ***MICROS Customer Support Remote Support Access Policy***.

Более подробно о Требовании **8** Стандарта **PCI DSS**, “Привязать уникальный идентификатор каждому, у кого есть доступ к ПК”, читайте вэб-сайт Совета **PCI SSC** https://www.pcisecuritystandards.org/

9. Ограничить физический доступ к данным держателей карт

Любой физический доступ к данным или системам с данными о держателях карт создает условия для доступа к устройствам или информации, с возможностью удалить систему или бумажную копию документа, и должен быть надлежащим образом ограничен.[11]

В соответствии со Стандартом **PCI DSS, MICROS Systems Inc.** настоятельно рекомендует ограничить физический доступ к данным о держателях карт. Входящий и исходящий трафик к средам данных о держателях карт должен быть ограничен.

Это касается также физического доступа к серверу торговой точки и любым компьютерным консолям, через которые возможен доступ к серверу торговой точки. Ограничивать надо также физический доступ к кредитным картам клиентов во время процедуры оплаты.

MICROS рекомендует ресторанам размещать свои серверы в закрытом на ключ помещении с ограниченным доступом и рекомендует официантам использовать ручные терминалы для оплат кредитными картами, так чтобы оплата завершалась у столика, а кредитная карта все время находилась в поле зрения ее владельца.

MICROS Systems, Inc. настаивает на том, чтобы пользователи не хранили данные о держателях карт в системах, доступных через интернет. Для обеспечения этого, сетевой сервер и сервер с данными должны быть разными.
Чтобы убедиться в том, что ваш сайт соответствует Требованию **9** Стандарта **PCI DSS, "**Ограничить физический доступ к данным о держателях карт**",** читайте вэб-сайт Совета **PCI SSC** https://www.pcisecuritystandards.org/

Регулярный мониторинг и тестирование сети

10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт

Механизмы ведения записей о событиях, а также возможность отслеживать действия пользователей совершенно необходимы. Наличие записей во всех средах позволяет провести тщательное расследование и проанализировать инциденты. Определить причину инцидентов, если отсутствуют записи событий, очень трудно.[12]

В **RES** заводится аудиторский журнал **(MICROS Security Log),** в котором записываются все действия, связанные с программированием безопасности данных о держателях кредитных карт, все доступы к данным о держателях кредитных карт и все действия под администратором **POS. MICROS** рекомендует держать этот журнал включенным и хранить архив, по меньшей мере, **1** год. Журнал безопасности **MICROS (MICROS Security Log)** включен по умолчанию, и его нельзя отключить. Для просмотра/работы с этим журналом, **о**ткройте **Microsoft Event Viewer (Windows Start | Control Panel | Administrative Tools)** и выберите **MICROS Security Log.**

11. "Payment Card Industry (PCI) Data Security Standard.doc", p. 11, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Для диагностики и решения проблем, а также на случай расследований, каждая рабочая станция записывает действия в отладочный **(debug)** лог-файл. Лог файл отладки всегда включен и не требует никаких действий со стороны торгово-сервисных предприятий, дилеров или специалистов по системной интеграции. Этот лог-файл находится здесь (если иное не указано пользователем): *\Micros\RES\POS\Etc*

Работающие объекты должны всегда держать журналы включенными на каждой рабочей станции. Этот файл отслеживает все действия, имеющие отношения к **POS** транзакциям.

Чтобы убедиться в том, что ваш сайт соответствует Требованию **10** Стандарта **PCI DSS**, "Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт", читайте вэб-сайт Совета **PCI SSC** https://www.pcisecuritystandards.org/

11. Регулярно тестировать системы и процессы информационной безопасности

Уязвимости то и дело обнаруживаются хакерами/разработчиками, а также появляются вместе с новыми программными продуктами. Системы, процессы и написанные на заказ программы необходимо часто тестировать, чтобы быть уверенными в их защищенности по мере того, как идет время и вносятся изменения [13]

В соответствии со Стандартом **PCI DSS, MICROS Systems Inc.** настоятельно рекомендует регулярно тестировать системы и процессы безопасности.

Чтобы убедиться в том, что настройки системы и процессов информационной безопасности настроены в соответствии с Требованием **11** Стандарта P**CI DSS**, "Регулярно тестировать системы и процессы информационной безопасности", читайте вэб-сайт Совета **PCI SS**C https://www.pcisecuritystandards.org/

Поддержание политики информа-ционной безопасности

12. Поддерживать политику информационной безопасности

Строгая политика информационной безопасности задает нужный тон в компании в целом и дает работникам представление о том, что от них ожидается. Все работники должны быть осведомлены о конфиденциальности данных и своей ответственности по их защите.[14]

В соответствии со Стандартом **PCI DSS, MICROS Systems Inc.** настаивает на поддержании политики информационной безопасности.

12. "Payment Card Industry (PCI) Data Security Standard.doc", p. 12, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.
13. "Payment Card Industry (PCI) Data Security Standard.doc", p. 13, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.
14. "Payment Card Industry (PCI) Data Security Standard.doc", p. 14, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Поддерживаемая на объекте политика информацинной безопасности должна включать информацию о физической безопасности, безопасности хранения и передачи данных, и об администрировании системы.

Политика Программного Обновления MICROS

MICROS Systems, Inc. может периодически предоставлять обновления программы **RES** удаленно. В этой связи, каждый объект должен разработать для своих работников политику обращения с критическими технологиями **(**например, технологии удаленного доступа, беспроводные технологии, съемные электронные носители, ноутбуки, персональные цифровые помощники **(PDA)**, **e-mail** и интернет**)**, чтобы обеспечить надлежащее использование этих технологий всеми работниками и подрядчиками.

Убедитесь в том, что эта политика включает следующие требования:

- Наличие четкого разрешение со стороны руководства на использование устройств с критическими технологиями.
- Предоставление доступа ко всем устройствам только при условии ввода имени пользователя и пароля или другого средства аутентификации **(**например, токен**)**.
- Наличие списка всех устройств и работников, авторизованных для работы с устройствами.
- Маркировка устройств с указанием ответственного, контактной информации и цели.
- Приемлемое использование технологий.
- Приемлемые местонахождения технологий на сети
- Наличие списка продуктов, утвержденных компанией.
- Автоматическое отключение модемных сессий после предопределенного периода неактивности
- Активация модемов, только при необходимости их использования поставщиками, с немедленной деактивацией после использования.
- Запрет на хранение данных о держателях карт на локальных или мягких **(floppy)** дисках, или других внешних носителях при обращении к таким данным удаленно через модем
- Запрет на удаленный доступ к функциям печати и вырезать-вставить.

MICROS Systems, Inc. рекомендует всем клиентам и дилерам**/**специалистам по системной интеграции использовать персональные межсетевые экраны при **VPN** или другом высоко-скоростном подключении, чтобы обезопасить эти “постоянные” **со**единения и обеспечить соответствие стандартам **PCI DSS**, изложенным на стр.**6**.

Чтобы убедиться в том, что ваша политика информационной безопасности настроена в соответствии с Требованием **12** Стандарта **PCI DSS, «**Поддерживать политику информационной безопасоности**»,** читайте вэб-сайт Совета **PCI SS**C https://www.pcisecuritystandards.org/

Проверочный лист безопасности данных кредитных карт

Этот проверочный лист должен обговариваться с клиентом и заполняться компанией-установщиком в подтверждение того, что надлежащие процедуры безопасности данных кредитных карт согласованы с клиентом.

Установлена версия программного обеспечения RES _____
Установлен драйвер кредитных карт _____
Установлена версия драйвера кредитных карт _____

	Да/Нет	Комментарии
Убедиться в наличии должным образом сконфигуренного межсетевого экрана.		
Убедиться в том, ч то выбраны опции Tender/Media для сокрытия Номера кредитной карты, Имени держателя кредитной карты и Даты окончания срока действия карты - для всех кредитных карт.		
Убедиться в том, что дефолтовые пароли на вход в операционную систему изменены.		
Убедиться в том, что дефолтовые пароли, заданные поставщиком, изменены.		
Убедиться в том, что точки доступа используют комплексные пароли, и что эти пароли, имевшие прежде дефолтовые значения, теперь изменены.		
Убедиться в том, что настройки комплексных паролей находятся в соответствии с требованиями PCI, и что у каждого пользователя есть свой уникальный идентификатор пользователя.		
Убедиться в том, что анти-вирусоное программное обеспечение установлено и актуально. Убедиться в том, что существует план обновления анти-вирусной программы.		
Убедиться в том, что сервер RES находится в защищенном месте, и что физический доступ к нему ограничен.		
Убедиться в том, что Журнал Безопасности MICROS ведет учет изменений. Также удостовериться в том, что ведется надлежащая архивации данных Журнала.		

Агент или Представитель MICROS

Фамилия_____

Компания_____

Дата _____

Подпись_ _____

Торгово-сервисная организация

Фамилия_____

Компания_____

Дата _____

Подпись_____

Приложение A

MICROS не вправе за вас менять ваши пароли. В настоящем приложении содержится образец простой таблицы, которую можно использовать для отслеживания смены паролей.

Удаленный Доступ

Для оказания поддержки, поставщики могут подключаться удаленно к вашему серверу. Это подключение должно быть защищено комплексным паролем.

Метод	Имя польз.	Пароль	Дата замены

Windows

Каждый работник вашей организации также должен получить собственный идентификатор (логин) для входа в ОС **Windows.** Также, свой собственный идентификатор для входа в ОС **Windows** должен получить каждый поставщик.

Имя пользов.	Пароль	Дата замены

Работники с доступом к Приложениям RES

Каждый работник вашей организации, которому нужен доступ к этим приложениям, должен получить свой собственный идентификатор на вход в **RES.** Также, собственный идентификатор должен получить каждый поставщик.

Работник	Имя польз.	Пароль	Дата замены
MICROS Support			
Property Expert			
Manager			

Пользователи базы данных

Ваша база данных **RES** требует наличия двух учетных записей пользователя. Это учетная запись администратора базы данных **(DBA)** и учетная запись пользователя **MICROS**. Пароли этих учетных записей должны меняться каждые **90** дней. Каждый работник вашей организации, которому нужен прямой доступ к базе данных, должен получить свой собственный идентификатор **(**логин**)** на вход в базу данных, причем, глубина доступа должна быть ограничена необходимыми функциями. Также, собственный идентификатор должен получить каждый поставщик.

Имя пользов.	Пароль	Дата замены
DBA		
MICROS		

Шифрование Базы Данных

Шифрование данных происходит по трем направлениям. Шифруется база данных, сами данные и транспортировка данных. Шифрование базы данных и данных требует ввода фразы-пароля.

Требования службы Поддержки:
Эта фраза-пароль используется только для генерации рандомизированного ключа. После его замены, она больше не нужна.

Тип Шифрования	Дата Изменения