NOVARTIS

Минимальный перечень контролей по Информационной Безопасности для Третьих сторон[1]

Версия 3.0

Апрель 2022

[1] С Минимальным перечнем контролей по Информационной Безопасности для Третьих сторон можно ознакомиться на сайте: https://www.novartis.com/esg/reporting/codes-policies-and-guidelines

Минимальный перечень контролей по Информационной Безопасности для Третьих сторон[2]

1. Управление и Соблюдение требований

- Третья сторона обязана внедрить и поддерживать стратегию информационной безопасности в соответствии с отраслевой практикой и стандартами безопасности для защиты систем и сетевой инфраструктуры, а также конфиденциальности, целостности, доступности и устойчивости данных, как минимум в объеме, учитывающим требования, изложенные в настоящем документе.
- Третья сторона должна убедиться, что надлежащим образом назначено лицо, действующее от имени Третьей стороны и ответственное за обеспечение соблюдения технических и организационных требований к средствам защиты информации.
- Стратегия информационной безопасности Третьей стороны должна содержать систему управления информационными рисками, включая необходимые политики по управлению рисками, которые обеспечивают и поддерживают соответсвующий процесс.

2. Обеспечение непрерывности процессов

- Третьей стороной должны быть внедрены надлежащие планы по обеспечению бесперебойной работы и аварийному восстановлению для обеспечения своервременного восстановления ИТ-систем, которые используются для любых операций с данными в любой форме, поддерживающие услуги, предоставляемые Новартис, в случае наступления стихийного бедствия или другого события, которое может привести к существенному сбою.
- Третья сторона обязана обеспечить периодическую проверку и обновление своих планов аварийного восстановления для обеспечения их актуальности и эффективности.
- Третья сторона обязана обеспечить достаточную защиту от любых разрушительных кибератак и регулярные проверки технологий и процессов, используемых для резервного копирования и восстановления данных.

3. Обращение с носителями информации

- Третьей стороной должны быть установлены процедуры, описывающие порядок обращения с информацией и способы ее хранения, с целью обеспечения защиты информации от несанкционированного раскрытия или неправильного использования.
- Третья сторона обязана обеспечить конфиденциальность и безопасность в процессе утилизации носителей информации, которые более не требуются, в соответствии с применимыми процедурами и с заполнением надлежащей документации.
- Третья сторона обязана обеспечить защиту системной документации от несанкционированного доступа.

[2] Выражения, написанные с заглавной буквы, используемые в этом документе, имеют то же значение, что и в последней версии Кодекса взаимодействия с третьими лицами Новартис (доступно по адресу https://www.novartis.com/esg/reporting/ code-policies-and-guidelines), если они прямо не определены в прилагаемом Глоссарии, или если в соответствии с контекстом не требуется иное толкование. В настоящем документе ссылки на «Третью сторону» или «Третьи стороны» ограничиваются только теми третьими сторонами, которые подпадают под определение «Поставщиков» в Кодексе взаимодействия с третьими лицами Новартис.

4. Обмен данными

- Третья сторона обязана поддерживать конфиденциальность, целостность, доступность и устойчивость данных и систем, на которых размещены или через которые доступны такие данные, в рамках своей организации и на внешнем объекте; это включает в себя наличие соглашения об обмене, защиту физических носителей при передаче, безопасный способ отправки электронных сообщений и защиту информации, которая обрабатывается корпоративными информационными системами.

5. Контроль доступа

- Третьей стороной должна быть установлена политика контроля доступа, гарантирующая, что доступ к данным Новартис получат только авторизованные пользователи, имеющие соответствующее разрешение и служебную необходимость.

- Третья сторона обязана регулярно проводить оценку прав доступа пользователей к данным Новартис и системам, хранящим такие данные, с целью обеспечения контроля за доступом, включая проверку обоснованности такого доступа, и, при необходимости, его ограничение.

6. Криптографическая защита информации

- Третьей стороной должна быть разработана и внедрена политика использования криптографических средств для надлежащей защиты данных, обеспечивающая при этом соблюдение применимых законодательных, нормативных и договорных требований.

7. Защиты коммуникаций и Сетевая безопасность

- Третья сторона обязана обеспечить надлежащее управление, контроль и защиту сетей, находящихся под контролем Третьей стороны, от угроз и уязвимостей, а также поддерживать конфиденциальность, целостность и доступность данных и предотвращать несанкционированный доступ к системам и приложениям, используемым для обработки данных в процессе хранения или передачи.

8. Обучение и информирование по вопросам безопасности

- Третья сторона обязана обеспечить информирование всех своих Сотрудников, представителей подрядчиков и посредников об угрозах и вопросах информационной безопасности, об их обязанностях и ответственности, а также предоставить набор инструментов для соблюдения принципов политики безопасности в своей работе.
- Третья сторона обеспечивает прохождение Сотрудниками, представителями подрядчиков и посредниками соответствующих обучающих курсов по вопросам информационной безопасности и защиты данных.
- Третья сторона обязана обеспечить использование Сотрудниками только корпоративных адресов электронной почты для любой корреспонденции, содержащей данные Новартис или относящейся к ним (вместо того, чтобы использовать личные адреса электронной почты или учетные записи платформ для обмена сообщениями).

9. Физическая безопасность и Безопасность среды

- Третья сторона обязана обеспечить наличие соответствующих периметров информационной безопасности и контроль за доступом для предотвращения

несанкционированного физического доступа, нанесения ущерба имуществу и информации Третьей стороны, включая все оборудование конечных пользователей.
- Третья сторона обязана обеспечить надлежащую инвентаризацию и обслуживание оборудования для соблюдения принципов информационной безопасности.

10. Защита документации организации

- Стратегия информационной безопасности Третьей стороны должна включать в себя политики, касающиеся хранения и уничтожения данных в соответствии с принятой отраслевой практикой.
- Третья сторона обязана обеспечить внедрение надлежащих средств контроля для предотвращения потери, уничтожения или фальсификации документации организации в течение срока ее хранения.
- Третья сторона обязуется по запросу Новартис или для выполнения требований законодательства ликвидировать (например, удалить, уничтожить или сделать не подлежащими прочтению) все данные Новартис, которые хранятся у Третьей стороны, ее аффилированных лиц или субподрядчиков (за исключением каких-либо копий данных Новартис на стандартных резервных носителях Третьей стороны при условии, что такие резервные носители будут защищены в соответствии с признанными и действующими методами в области защиты персональных данных и принятой отраслевой практикой). Третья сторона обязуется предоставить Новартис по запросу подробный отчет по данным, хранящимся на резервных носителях, без дополнительных затрат для Новартис. Новартис оставляет за собой право на получение копии данных Новартис в форме и в определенные Новартис сроки перед их уничтожением.
- По запросу Новартис Третья сторона обязуется в письменной форме предоставить подтверждение о выполненных операциях.
- Следующие случаи являются исключениями из этого требования о ликвидации:
  - Третья сторона обязана хранить данные Новартис для юридических или нормативных целей; такие данные Новартис должны быть удалены после истечения установленных законом сроков хранения.
  - Данные Новартис, которые Третья сторона обязана сохранить без изменений по требованию Новартис для целей, связанных с судебными разбирательствами и другими юридическими причинами.
  - В случае, если в письменной форме между Новартис и Третьей стороной согласованы конкретные требования по возврату/уничтожению/сохранению определенных данных Новартис, то такие требования должны быть соблюдены.

11. Управление техническими уязвимостями

- Третьей стороной должна быть внедрена стратегия управления уязвимостями, которая отслеживает статус и поддерживает уровень информационной безопасности в ИТ-среде Третьей стороны.
- Третья сторона обязана внедрить и поддерживать политики, демонстрирующие надлежащее применение и управление обновлениями и исправлениями в ИТ-системах Третьей стороны.
- Третья сторона обязана иметь в наличии и поддерживать реестр аппаратного и программного обеспечения и проводить регулярные сканирования уязвимостей.

12. Управление инцидентами информационной безопасности

- Третья сторона обязана установить ответственность и процедуры, которые обеспечивают быстрое и своевременное реагирование на инциденты информационной безопасности, а также определяют порядок информирования, управления и формирования отчетности по инцидентам и слабым местам в области информационной безопасности.

- Третья сторона обязана незамедлительно проинформировать Новартис в случае возникновения инцидента безопасности, связанного с данными Новартис.

13. Мониторинг

- Третья сторона обязана проводить мониторинг своей среды для обнаружения и реагирования на инциденты информационной безопасности или на другие несанкционированные действия.
- Третья сторона обязана использовать средства аудиторского контроля в среде под управлением Третьей стороны, которые обеспечивают независимый аудит / оценку соответствующих данных аудиторского контроля в операционных системах с сокращением до минимума риска нарушения процессов бизнеса.

14. Управление конфигурацией и изменениями

- Третьей стороной должен быть установлен процесс управления изменениями, который учитывает этап оценки влияния изменений до их внедрения, включает критерии для определения эффективности или неэффективности изменения и обеспечивает согласование процедуры отмены неэффективных изменений до осуществления изменений.

15. Защита от воздействия вредоносных кодов

- Третья сторона обязана разработать политики управления рисками, связанными с распространением вредоносного кода, и внедрить средства защиты от вредоносных программ.