Дополнительные требования к информационной безопасности

Настоящие Дополнительные требования к защите информации («AISR») дополняют любые другие требования к защите информации, содержащиеся в Соглашении, Кодексе взаимодействия с третьими лицами Новартис («TPC») и Минимальном наборе требований к средствам защиты информации («MISC»).

1. **Оценки и сертификаты информационной безопасности (дополняет раздел 12.5 TPC)**
   - 1.1 Компания Новартис или уполномоченная третья сторона может проводить технические и/или другие оценки, включая тестирование для оценки безопасности и степени устойчивости элементов для Данных Новартис и Среды Новартис.
   - 1.2 Третья сторона и ее субподрядчики обязуются поддерживать сертификаты безопасности, указанные в Договоре и проходить независимые аудиты.
   - 1.3 Третья сторона обеспечивает периодическое (не реже одного раза в год) проведение опытными и квалифицированными специалистами тестов на проникновение и безопасность в соответствии с Принятой отраслевой практикой для среды, в которой обрабатываются Данные Новартис, а результаты таких тестов предоставлять Новартис по запросу.
   - 1.4 Что касается разделов 1.1-1.3 выше, то при обнаружении каких-либо уязвимостей или отклонений, Третья сторона обязуется без избыточного промедления подготовить план корректирующих мер и выполнить указанные в плане действия, в соответствии с Принятой отраслевой практикой. Невыполнение Третьей стороной этого требования дает компании Новартис право расторгнуть Соглашение согласно соответствующему пункту о расторжении Соглашения.

2. **Общие требования к информационной безопасности (дополняет разделы 1, 3, 5 и 6 MISC)**
   - 2.1 Третья сторона обязуется обрабатывать Данные Новартис в соответствии с Принятой отраслевой практикой.
   - 2.2 Стратегия информационной безопасности Третьей стороны периодически (не реже одного раза в год) пересматривается и обновляется на основе оценок, касающихся: (i) внутренних и внешних рисков; (ii) использования защитной инфраструктуры или процессов управления; (iii) способности обнаруживать угрозы, реагировать на них и смягчать их; и (iv) соответствия требованиям законодательства.
   - 2.3 Принимая во внимание соответствующие риски информационной безопасности, Третья сторона обязуется внедрить надлежащий(е) стандарт(ы) шифрования в соответствии с Общепринятыми стандартами информационной безопасности, например, как минимум NIST 800 и/или ISO 27001.
   - 2.4 Третья сторона обеспечивает наличие многофакторной аутентификации для систем, содержащих Данные Новартис и использующих сеть общего доступа, а также для доступа к среде Третьей стороны (где обрабатываются данные Новартис) с рабочих станций пользователей Третьей стороны.
   - 2.5 Третья сторона обязуется обрабатывать Данные Новартис только в: (a) безопасной Рабочей среде; или (b) любой другой взаимно согласованной среде, которая является безопасной.
   - 2.6 Третья сторона обязуется в соответствии с предоставляемыми услугами внедрять и поддерживать меры, соответствующие Принятой отраслевой практике, для обнаружения, расследований, устранения и предотвращения проникновений, применения или выполнения любого несанкционированного или вредоносного кода, который каким-либо образом может повлиять на безопасность Данных Новартис или Среды Новартис.

2.7 Третья сторона обязуется отслеживать доступные исправления, оценивать, тестировать и своевременно внедрять их для любых систем, участвующих в обработке Данных Новартис.

2.8 Третья сторона обязуется вести соответствующие журналы событий для поддержки аудитов безопасности, а также для обнаружения и расследования любого Инцидента безопасности.

3. <u>Стандарты непрерывности деятельности (дополняет раздел 12.9 TPC и раздел 2 MISC)</u>

3.1 Третья сторона обеспечивает Целевое время восстановления (RTO) и Целевую точку восстановления (RPO), указанные в таблице ниже (в зависимоти от классификации по Доступности применяется один из вариантов – Высокий или Средний):

Цель (Доступность приложений/системы – Высокая)	Максимальное время для достижения цели [в часах]
Целевое время восстановления (RTO)	24 (или если не предусмотрено иное в соответствующем Техническом задании/Заказе на поставку)
Целевые точки восстановления (RPO)	8 (или если не предусмотрено иное в соответствующем Техническом задании/Заказе на поставку)
Цель (Доступность приложений/системы – Средняя)	Максимальное время для достижения цели [в часах]
Целевое время восстановления (RTO)	72 (или если не предусмотрено иное в соответствующем Техническом задании/Заказе на поставку)
Целевые точки восстановления (RPO)	24 (или если не предусмотрено иное в соответствующем Техническом задании/Заказе на поставку)

4. <u>Среда Новартис (дополняет разделы 4, 7 и 8 MISC)</u>

4.1 Любое подключение к Среде Новартис, включая параметры подключения, требует предварительного одобрения Новартис и соответствия Третьей стороны требованиям Новартис и может быть отключено Новартис в любое время.

4.2 Если сотрудники Третьей стороны получат: (i) пропуск компании Новартис или другое средство доступа; (ii) персонализированную учетную запись для доступа в сеть компании Новартис; (iii) устройство Новартис; (iv) учетную запись электронной почты Новартис, или (v) другой доступ к Среде Новартис, то Третья сторона обязуется обеспечить соблюдение такими сотрудниками применимых политик информационной безопасности Новартис. Третья сторона обязуется сообщать Новартис о любых изменениях в организационной структуре, которые могут повлиять на Новартис. Третья сторона также обязуется обеспечить контроль за соблюдением применимых политики и стандартов информационной безопасности сотрудниками, которые имеют доступ к среде Третьей стороны, содержащей Данные Новартис.

5. <u>Инциденты безопасности (дополняет раздел 12 MISC)</u>

5.1 Третья сторона отслеживает Инциденты безопасности, анализирует их и реагирует на них.

5.2 Третья сторона обязуется уведомить Новартис об Инциденте безопасности без излишнего промедления, но не позднее, чем через двадцать четыре (24) часа после того, как стало известно об инциденте.

5.3 Контакты Новартис для сообщения об Инциденте безопасности: Телефон: +420 225 775 050 (дополнительный номер: +420 225 850 012), электронная почта: soc@novartis.com

5.4 Третья сторона обязуется незамедлительно по запросу Новартис предоставить контакт для сообщения или обсуждения Инцидента безопасности.

5.5 В случае обнаружения Инцидента безопасности, Третья сторона обязуется без излишнего промедления предпринять соответствующие действия для сведения к минимуму дальнейшего раскрытия Данных Новартис и принять восстановительные меры, чтобы предотвратить повторение подобного Инцидента безопасности.

5.6 Третья сторона обязуется сообщить об основных причинах Инцидента безопасности и воздействии на Данные Новартис, а также о ходе выполнения принятых восстановительных действий.

6. Требования к использованию системы искусственного интеллекта (в дополнение к разделу 7 MISC). (Примечание при составлении проекта договора: Этот раздел применим только к классификации AI – Высокий риск.) Третья сторона должна, как минимум, поддерживать следующие меры безопасности при обработке Данных Новартис с помощью систем искусственного интеллекта:

6.1 Наборы данных, применяемые в области ИИ, включающие Данные Новартис, управляются надлежащим образом, и их право собственности определяется в момент владения таким набором данных ИИ Третьей стороной. Наборы данных ИИ, включающие данные Новартис, являются полными, точными и безопасными. Данные шифруются там, где это необходимо, вводимые данные проверяются и безопасно удаляются, а любые персональные данные, используемые для обучения ИИ, анонимизируются. После получения предварительного письменного разрешения Новартис, для случаев, когда данные Новартис используются для обучения систем ИИ Третьей стороны, принимаются соответствующие меры для обеспечения безопасности, целостности и доступности данных Новартис.

6.2 Для интерактивных информационных системы, случаи взаимодействия с системой ИИ регистрируются. Доступ к журналам событий ограничен соответствующими ролями. Взаимодействие ИИ систем отслеживается, и принимаются меры для обнаружения атак внедрения запроса и/или любых других атак, специфичных для ИИ.

6.3 Тестирование ИИ систем на проникновение включает в себя векторы атак, специфичные для ИИ (например, внедрение запроса, джейлбрейк, извлечение данных, контролируемое отравление обучающих данных).

6.4 Для обнаружения и фильтрации потенциально чувствительных данных в запросах, отправленных пользователем, и загруженных пользователем документах, применяются меры по предотвращению потери данных, проектирование запросов и проверка вводимых данных.

6.5 История чата и загруженные пользователем файлы надлежащим образом защищены и, где это применимо, позволяют пользователям периодически очищать историю в соответствии с политикой хранения.

6.6 Для интерактивных информационных системы предусмотрены мероприятия для обнаружения ботов, гарантирующие, что с ИИ системой взаимодействуют только пользователи-люди. Выходные данные ИИ системы периодически проверяются на предмет выявления неточностей (например, предвзятости в ответах, недостоверной информации), а

также потенциальной утечки конфиденциальной информации или интеллектуальной собственности. Модели ИИ обновляются на основе периодических проверок и других входных данных, чтобы улучшить понимание вредоносных запросов и пограничных случаев.

ОПРЕДЕЛЕНИЯ [Примечание: приведенные ниже определения следует скорректировать, чтобы они соответствовали конкретному контракту.]

Приведенные ниже определения относятся к терминам, написанным с заглавной буквы, которые используются в настоящем AISR.

«Данные Новартис» - все данные, информация, документы или записи любого характера (включая персональные данные и конфиденциальную информацию Новартис) в любой форме, независимо от того, существовали ли они до или после даты Соглашения, были ли созданы или обработаны Третьей стороной в связи с услугами, предоставляемыми для Новартис или предоставляемыми от Новартис (или третьими сторонами, действующими от имени Новартис) Третьей стороне в рамках Соглашения.

«Среда Новартис» - любая система или инфраструктура Новартис, управляемая Новартис или от имени Новартис, Аффилированными лицами Новартис или субподрядчиком Новартис, доступная для Третьей стороны.

«TPC» - Кодекс взаимодействия с третьими лицами Новартис, упомянутый в Соглашении.

«MISC» – Минимальный набор требований к средствам защиты информации Новартис, опубликованные на общедоступном сайте Новартис: https://www.novartis.com/esg/reporting/codes-policies-and-guidelines и являющийся частью TPC.

«Рабочая среда» - среда, в которой готовое программное обеспечение, продукты или обновления выпускаются для эксплуатации предполагаемыми конечными пользователями.

«Целевая точка восстановления (RPO)» означает, какой объем Данных Новартис может быть потерян без возможности восстановления.

«Целевое время восстановления (RTO)» означает, как долго услуги, Данные Новартис или системы, используемые для предоставления услуг в соответствии с Соглашением, могут быть недоступны.

«Инцидент безопасности» - событие, которое фактически или потенциально ставит под угрозу конфиденциальность, целостность или доступность Данных Новартис или иным образом ставит под угрозу информационную безопасность Среды Новартис.

«Принятая отраслевая практика» - соответствующие отраслевые стандарты и практики, повсеместно принятые в сфере информационной безопасности, для компаний, сопоставимых с Третьей стороной, и/или компаний, обрабатывающих сопоставимую информацию, закрепленные в различных отраслевых стандартах, предоставляемых Международной организацией по стандартизации (ISO/IEC) ISO/IEC ISO27001, ISO/IEC 27002:2013, SSAE-18, ISAE3402, Национальным институтом стандартов и технологий (NIST) NIST 800-55, Руководством по созданию безопасных веб-

приложений Open Web Application Security Project (OWASP), Центром интернет-безопасности (CIS) (или любым общепринятым преемником таких стандартов безопасности) и в других стандартах, относящихся к области действия предмета Соглашения.