**ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

|  |  |
| --- | --- |
| **Про этот документ** Для целей иллюстрации – можно удалить перед подписанием | |
| * Настоящее положение предусмотрено для использования в качестве приложения к основному договору, реквизиты которого необходимо указать в преамбуле. | * В положении определены системы заказчика, к которым исполнитель получает доступ (п. 2.1). * Определены правила использования систем заказчика (п. 2.2). |
| * Положение содержит правила, которые исполнитель по основному договору должен соблюдать при работе с системами и данными заказчика (например, заказчик предоставляет разработчику доступ на свой сервер). | * Данные заказчика, в том числе расположенные в его системах, являются конфиденциальной информацией (п. 3 и п. 4). * Исполнитель обязан следить за безопасностью своих систем (п. 5). |
| * В случае нарушения положения заказчик имеет право расторгнуть основной договор (п. 10) и потребовать возместить убытки, вызванные несоблюдением положения (п. 11). | * Исполнитель обязан соблюдать меры реагирования на нарушение безопасности (п. 6). * Исполнитель обязан проводить ежегодный аудит своих систем (п. 8). |
| * Исполнитель несет ответственность только при наличии вины в форме прямого или косвенного умысла или неосторожности. | * Исполнитель должен разработать программу информационной безопасности (п. 9). |
| Настоящий шаблон разработан юристами Buzko Krasnov. Не является юридической консультацией. Обязательно проконсультируйтесь со своим юристом перед использованием документа.  Этот шаблон входит в состав пакета юридических документов для разработчиков игр и ПО. Актуальная версия документов на нашем сайте по этой ссылке: <https://www.buzko.legal/digital/yuridicheskie-dokumenty-dlya-razrabotchikov-igr-i-po>. | |

Настоящее Положение об информационной безопасности («**Положение**») является юридически обязывающим приложением к договору [реквизиты договора] («**Договор**»), заключенному между:

1. [**Наименование**], юридическим лицом, созданным и действующим в соответствии с законодательством Российской Федерации, с местом нахождения по адресу: [xxx], ОГРН [xxx] («**Заказчик**»), в лице генерального директора [xxx], действующего на основании устава Заказчика, и
2. [**ФИО**], паспорт гражданина Российской Федерации номер [xxx], с регистрацией по адресу: [Российская Федерация, г. Москва] («**Исполнитель**»),

далее совместно именуемые «**Стороны**», а каждый в отдельности – «**Сторона**».

**СТОРОНЫ ДОГОВОРИЛИСЬ О НИЖЕСЛЕДУЮЩЕМ:**

1. **ПРЕДМЕТ**
   1. **Предмет Положения**. Настоящее Положение определяет меры информационной безопасности, которые Стороны должны соблюдать в рамках их взаимодействия по Договору в целях недопущения нарушения информационной безопасности.
   2. **Нарушение информационной безопасности**. Нарушением информационной безопасности является случайное или незаконное уничтожение, потеря, изменение, несанкционированное раскрытие или доступ к Системам Заказчика или к Данным Заказчика (как эти термины определены ниже), вызванное или возникшее в том числе в результате сбоя, нарушения, кибератаки, отсутствия или несоответствия информационной безопасности, физического вторжения в помещения, кража или потеря документов, компьютеров, устройств или носителей информации, а также должностные преступления сотрудников или подрядчиков Исполнителя, которые произошли по вине или в результате неосторожности Исполнителя.
2. **ДОСТУП К СИСТЕМАМ ЗАКАЗЧИКА**
   1. **Системы Заказчика**. Если Заказчик предоставляет Исполнителю доступ к используемым Заказчиком системам, то есть к:
      1. компьютеру, в том числе виртуальной машине;
      2. компьютерной сети;
      3. серверам, в том числе виртуальным;
      4. контейнерам, виртуальным окружениям или их аналогам;
      5. базам данных;
      6. программному обеспечению;
      7. сервисам, в том числе облачным и прочим, администрируемым Заказчиком или третьими лицами;
      8. запоминающему устройству;
      9. мобильному устройству; или
      10. к иному оборудованию, программному обеспечению или сетям, которые принадлежат на праве собственности, аренды или контролируются (используются) Заказчиком или его аффилированными лицами или управляются третьей стороной от имени или для Заказчика;

(далее совместно «**Системы Заказчика**»),

Исполнитель обязан соблюдать определенные меры информационной безопасности в соответствии с данным Положением.

* 1. **Использование Систем Заказчика**. При использовании Систем Заказчика Исполнитель (включая его сотрудников, подрядчиков и контрагентов) обязан:
     1. Использовать зашифрованное соединение;
     2. Не использовать публичный Wi-Fi (даже если он защищен паролем). Исключение – подключение с доверенным VPN (риск потери данных или иной компрометации в этом случае лежит на Исполнителе, как лице, обязанном использовать доверенный сервис VPN);
     3. Использовать стойкие пароли в соответствии с пунктом 7 Положения;
     4. Использовать двухфакторную авторизацию, если такая возможность предусмотрена конкретной Системой Заказчика;
     5. Использовать со своей стороны исключительно официальное программное обеспечение (не «пиратские» версии), а также обновлять его до последней версии;
     6. Использовать со своей стороны антивирусное программное обеспечение;
     7. Ограничить доступ к Системам Заказчика и предоставлять его исключительно своим сотрудникам, подрядчикам и контрагентам, если такой доступ им необходим для исполнения Договора;
     8. Отслеживать и сообщать Заказчику в течение 1 часа после обнаружения о несанкционированном доступе к Системам Заказчика посредством данных, предоставленных Исполнителю для авторизации в Системах Заказчика или их использования, преимущественно перед иными мерами реагирования в соответствии с пунктом 6 Положения;
     9. Не разглашать третьим лицам информацию об использовании Заказчиком определенных Систем Заказчика и тех или иных элементов в Системах Заказчика, включая оборудование, программное обеспечение, их настройки, конфигурации, IP-адреса, доменные имена и пр.
  2. **Отзыв доступа к Системам Заказчика**. Заказчик в любой момент по любой причине и без предупреждения может ограничить доступ Исполнителя к Системам Заказчика. В этом случае если Исполнитель не может продолжать осуществлять свои обязанности по Договору из-за такого ограничения, Исполнитель не несет ответственности за неисполнение или ненадлежащее исполнение своих обязательств по Договору. При этом Исполнитель обязан своевременно возобновить исполнение своих обязательств по Договор по возобновлению доступа к Системам Заказчикам.
  3. **Права на Системы Заказчика**. Права на Системы Заказчика ни в каком случае не переходят Исполнителю.

1. **ДАННЫЕ ЗАКАЗЧИКА, ИХ ИСПОЛЬЗОВАНИЕ И ПРАВА НА НИХ**
   1. **Данные Заказчика**. Во время исполнения Договора Исполнитель может получать доступ к данным Заказчика. Такими данными являются:
      1. данные, расположенные в Системах Заказчика или данные, доступ к которым можно получить с помощью Систем Заказчика;
      2. данные, предоставленные Заказчиком Исполнителю иным образом, например, лично, через email или по почте, а также устно;

(далее совместно «**Данные Заказчика**»).

* 1. **Состав Данных Заказчика**. Данные Заказчика содержат в том числе любую информацию и материалы, предоставленные Заказчиком, его материнской компанией, филиалами, дочерними компаниями, подрядчиками, субподрядчиками, директорами, сотрудниками, агентами, представителями, клиентами, аффилированными лицами и включают, помимо прочего, информацию:
     1. о Системах Заказчика (конфигурация, используемое оборудование, используемое программное обеспечение, IP-адреса, доменные имена и пр.);
     2. логины, пароли, коды доступа и тому подобное;
     3. о программном обеспечении и документации к ней;
     4. о коммерческой деятельности;
     5. об организационной структуре;
     6. об интеллектуальной собственности;
     7. об имущественных правах;
     8. о правой и иной документации;
     9. информацию, касающуюся бизнес-планов (стратегических, тактических и прочих);
     10. информацию относительно маркетинга, промо или рекламной деятельности;
     11. дизайн или проект чего-либо;
     12. о ценовой политике;
     13. персональные данные;
     14. конфиденциальная информация (являющаяся таковой в силу закона или любого договора);
     15. ранее произведенные или оказанные, существующие или будущие продукты или услуги (включая спецификации и проекты);
     16. процессы, процедуры и методологии (например, технические, логистические или инженерные процедуры);
     17. ноу-хау;
     18. доменные имена;
     19. IP-адреса; и
     20. различные отчеты, анализы, аналитика;
     21. содержание настоящего Положения.
  2. **Использование Данных Заказчика**.Исполнитель имеет право использовать Данные Заказчика исключительно для целей исполнения своих обязательств по Договору.
  3. **Права на Данные Заказчика**. Права на Данные Заказчика ни в каком случае не передаются и не переходят Исполнителю. Любые данные или информация, созданные на основе Данных Заказчика, также являются собственностью Заказчика и не переходят Исполнителю.

1. **КОНФИДЕНЦИАЛЬНОСТЬ ПОЛОЖЕНИЯ И ДАННЫХ ЗАКАЗЧИКА**
   1. **Конфиденциальная информация**. Стороны настоящим согласовали, что Данные Заказчика, настоящее Положение и связанная с ним информация являются конфиденциальной информацией («**Конфиденциальная информация**»). Исполнитель обязуется сохранять конфиденциальность такой информации (в том числе принимать меры для ее охраны, не разглашать и не использовать в своих личных целях или иным несоответствующим образом), за исключением случаев, когда такая информация:
      1. Является общеизвестной и стала таковой не в связи с нарушением Исполнителем положений Договора или Положения;
      2. Должна быть раскрыта в соответствии с императивными положениями применимого права или предоставлена государственному органу по его требованию с учетом особенностей, указанных ниже в пункте 4.5 Положения;
      3. Получена Исполнителем или его аффилированными лицами из официальных или иных публично открытых и доступных источников при условии, что конфиденциальная информация попала в такие источники не в связи с нарушением Исполнителем или его аффилированными лицами положений Договора или Положения;
      4. Раскрывается Исполнителем третьему лицу в той степени, в которой такое раскрытие необходимо в целях исполнения обязательств Исполнителя по Договору с учетом особенностей, указанных ниже в пунктах 4.3 и 4.4 Положения;
      5. Требуется Исполнителю для целей третейского разбирательства в соответствии с Договором, Положением или защиты иного права и интереса Исполнителя в судебном или административном порядке.
   2. **Охрана конфиденциальности**. Исполнитель должен принимать разумные меры по охране Конфиденциальной информации, в том числе путем соблюдения правил работы с Системами Заказчика и Системами Исполнителя.
   3. **Передача Конфиденциальной информации**. Исполнитель не имеет права разглашать или передавать кому-либо (в том числе своим подрядчикам) Конфиденциальную информацию без предварительного письменного разрешения Заказчика. Исполнитель не имеет права использовать Конфиденциальную информацию в своих личных целях или иным несоответствующим образом.
   4. **Условие передачи Конфиденциальной информации**. Если Исполнитель передает Конфиденциальную информацию третьим лицам с разрешения Заказчика или в случаях, предусмотренных в пункте 4.1, он должен обеспечить, чтобы такие третьи лица приняли на себя обязательства о сохранении Конфиденциальной информации в тайне, а также о соблюдении мер по информационной безопасности на уровне, не ниже данного Положения.
   5. **Требования о раскрытии Конфиденциальной информации**. Если Исполнитель получает требование о раскрытии Конфиденциальной информации (в составе другой информации или исключительно ее) от суда, иного органа государственной власти или от органа (субъекта), исполнение которого является обязательным в силу закона, Исполнитель должен:
      1. В течение 1 рабочего дня сообщить об этом Заказчику, в том числе по электронной почте, с приложением соответствующего требования или иного документа об истребовании Конфиденциальной информации;
      2. Сделать все возможное в рамках закона, чтобы не передавать Конфиденциальную информацию, в том числе со ссылкой на их конфиденциальный характер и отсутствие необходимых прав для передачи информации. Расходы Исполнителя, возникшие в связи с этим, подлежат возмещению по предварительному согласованию с Заказчиком.
2. **СИСТЕМЫ ИСПОЛНИТЕЛЯ И ОБЛАЧНЫЕ СЕРВИСЫ**
   1. **Системы Исполнителя, поддержка их безопасности**.Понятие Систем Исполнителя определяется по аналогии с понятием Систем Заказчика (пункт 2.1 Положения) («**Системы Исполнителя**»). Исполнитель (включая его сотрудников и подрядчиков) должен следить и поддерживать информационную безопасность своих систем при их использовании и администрировании, в частности:
      1. Использовать зашифрованное соединение;
      2. Не использовать публичный Wi-Fi (даже если он с паролем). Исключение – подключение с доверенным VPN (риск потери данных или иной компрометации в этом случае лежит на Исполнителе, как лице, обязанном использовать доверенный сервис VPN);
      3. Использовать стойкие пароли в соответствии с пунктом 7 Положения;
      4. Использовать двухфакторную авторизацию, если такая возможность предусмотрена конкретной Системой Исполнителя;
      5. Использовать исключительно официальное программное обеспечение (не «пиратские» версии), а также обновлять его до последней версии;
      6. Использовать антивирусное программное обеспечение в составе Систем Исполнителя и на устройствах, которые работают с ними;
      7. Ограничить доступ к Системам Исполнителя и предоставлять его исключительно своим сотрудникам, подрядчикам, иным авторизованным лицам;
      8. Отслеживать и сообщать Заказчику в течение 1 часа после обнаружения о несанкционированном доступе к Системам Исполнителя;
      9. Насколько это возможно осуществлять физическую охрану Систем Исполнителя. Например, если конкретные Системы Исполнителя являются сервисами, которые предоставляются Исполнителю третьими лицами (в том числе облачные сервисы), их физической охраной Исполнитель заниматься не должен.
   2. **Облачные сервисы Исполнителя**.Если Исполнитель пользуется облачными и прочими сервисами, которые администрируются третьими лицами, Исполнитель имеет право работать с Данными Заказчика (хранить, передавать, обрабатывать их и тому подобное) в таких сервисах, только с согласия Заказчика. Настоящим такое согласие выдано в отношении следующих сервисов, которые используются Исполнителем:
      1. [название сервиса со ссылкой];
      2. [название сервиса со ссылкой]; и
      3. [название сервиса со ссылкой].
3. **МЕРЫ РЕАГИРОВАНИЯ НА НАРУШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, КОНФИДЕНЦИАЛЬНОСТИ**
   1. **Защита Систем Исполнителя**.Исполнитель должен прилагать все усилия, чтобы способствовать выявлению и предотвращению любых нарушений информационной безопасности Систем Исполнителя. В случае обнаружения нарушений информационной безопасности Исполнитель должен предпринять все необходимые действия по восстановлению безопасности Систем Исполнителя за счет собственных средств.
   2. **Меры реагирования на нарушения информационной безопасности**. В случае обнаружения нарушений информационной безопасности Систем Заказчика, Систем Исполнителя или разглашения, получения несанкционированного доступа к Конфиденциальной информации, а также в случае наличия обоснованных подозрений об этом, Исполнитель должен:
      1. Немедленно провести обоснованное расследование причин и обстоятельств, связанных с таким нарушением безопасности;
      2. Прилагать все усилия и предпринимать все необходимые действия для предотвращения и минимизации последствий такого нарушения безопасности;
      3. Направить Заказчику в кратчайшие возможные сроки, но в любом случае не позднее 6 часов с момента, когда Исполнитель обнаружил или обоснованно заподозрил такое нарушение безопасности, уведомление по электронной почту, телефону или иному каналу связи, позволяющему Исполнителю удостовериться в получении Заказчиком такого уведомления;
      4. Незамедлительно и ни в коем случае не позднее, чем через 48 часов с момента, когда Исполнитель обнаружил или обоснованно заподозрил нарушение безопасности, предоставить Заказчику письменный отчет о таком нарушении безопасности, включая список всех лиц, у которых есть или был доступ к Данным Заказчика и Системам Заказчика;
      5. Собирать и сохранять все доказательства, касающиеся обнаружения, причины, уязвимости, корректирующих действий и воздействия, связанных с таким нарушением безопасности.
   3. **Подозрения о нарушении информационной безопасности Исполнителя**. Если Заказчик уведомлен о каком-либо нарушении безопасности или иным образом обнаруживает или подозревает, что Исполнитель пострадал от нарушения безопасности, по запросу Заказчика Исполнитель должен предоставить Заказчику любые запрошенные Заказчиком документы, связанные с таким нарушением безопасности, включая, помимо прочего, любые отчеты об оценке безопасности и контроля безопасности, журналы и любой анализ такого нарушения безопасности (при их наличии).
   4. **Сотрудничество Исполнителя с Заказчиком**. Исполнитель будет сотрудничать с Заказчиком в поисках любого вида обеспечения защиты против лица, которое считается ответственным или соучастником нарушения безопасности.
4. **ТРЕБОВАНИЯ К ПАРОЛЯМ**
   1. **Стойкие пароли**. При работе с Системами Заказчика, Системами Исполнителя, Исполнитель должен использовать стойкие пароли. Пароли считаются стойкими, если они:
      1. имеют длину не менее 8 символов;
      2. не являются стандартными, например дата рождения, «12345678», «qwerty», «password» и т.д.;
      3. состоят из символов разного регистра (большие и маленькие буквы);
      4. включают в себя сочетание букв, цифр, а также специальных символов (например, «!», «@», «$» и др., если это допустимо в конкретной системе, сервисе);
      5. являются уникальными, то есть не используются Исполнителем в различных системах, сервисах (одна учетная запись (аккаунт) – один уникальный пароль);
      6. меняются не менее чем раз в [полгода];
      7. не разглашаются неуполномоченным лицам.
5. **АУДИТ ИСПОЛНИТЕЛЯ**
   1. **Ежегодный аудит Исполнителя**. Исполнитель обязуется ежегодно проводить аудит информационной безопасности в отношении Систем Исполнителя и его предприятия (бизнеса) в целом. Такой аудит может быть проведен собственными силами без привлечения третьей стороны. В случае привлечения для аудита третьей стороны, Заказчик не возмещает Исполнителю возникшие в этой связи расходы.
   2. **Аудит Исполнителя от Заказчика**. По собственному усмотрению и за свой счет Заказчик может проводить не чаще чем раз в год аудит Систем Исполнителя и его предприятия (бизнеса) на предмет информационной безопасности. Такой аудит может быть проведен Заказчиком самостоятельно или с привлечением третьего лица. Исполнитель не должен препятствовать проведению такого аудита и обязан оказать содействие.
6. **ПРОГРАММА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**
   1. **Программа информационной безопасности**.Исполнитель должен иметь (или разработать) и соблюдать программу информационной безопасности – документ (например, в качестве локального нормативного акта), регламентирующий технические и организационные меры, соблюдение которых позволит поддерживать уровень информационной безопасности при ведении Исполнителем своей деятельности на уровне, не ниже установленном данным Положением («**Программа информационной безопасности**» или «**ПИБ**»).
   2. **Доступ к ПИБ**. Заказчик имеет право ознакомиться с ПИБ Исполнителя.
7. **ПРИОСТАНОВКА ИСПОЛНЕНИЯ И РАСТОРЖЕНИЕ ДОГОВОРА**
   1. **Право Заказчика приостановить исполнение Договора**. Несоблюдение настоящего Положения является основанием для приостановки исполнения Заказчиком своих обязательств по Договору. В этом случае Заказчик должен направить Исполнителю соответствующее уведомление не позднее, чем за 3 календарных дня до предполагаемой даты приостановки исполнения Договора.
   2. **Право Заказчика расторгнуть Договор**. Если основания, указанные в пункте 10.1 Положения, сохраняются в течение 15 календарных дней, Заказчик имеет право расторгнуть Договор в одностороннем порядке без уплаты каких-либо штрафных санкций.
8. **ОТВЕТСТВЕННОСТЬ СТОРОН**
   1. **Основание для привлечения Исполнителя к ответственности**. В дополнение к любым обязательствам по возмещению убытков, содержащимся в других частях Договора, Исполнитель соглашается возместить Заказчику убытки, возникающие в результате:
      1. любого нарушения настоящего Положения;
      2. любого несоблюдения Исполнителем (его сотрудниками, подрядчиками и контрагентами) каких-либо законов, нормативных актов, применимых к Исполнителю, в отношении информационной безопасности или конфиденциальности.
   2. **Условия привлечения Исполнителя к ответственности**. Ответственность Исполнителя, вытекающая из данного Положения, налагается на него исключительно при наличии вины Исполнителя в форме прямого или косвенного умысла или неосторожности.
9. **ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**
   1. **Применимое право**. Положение регулируется правом Российской Федерации.
   2. **Термины**. Термины, начинающиеся с заглавной буквы, имеют определенное значение, данное такому термину в тексте Положения («**Пример термина**»).
   3. **Толкование Положения**. Если иное не вытекает из контекста Положения, при его толковании необходимо учитывать следующее: (i) заголовки Положения не имеют юридического значения и даны для удобства восприятия текста; (ii) слова «включая», «включающий», «в том числе» рассматриваются без ограничения толкования перечисленным; (iii) слова, используемые в единственном числе, включают в себя и значение множественного числа, и наоборот.
   4. **Исчерпывающий характер**. Настоящее Положение представляет собой исчерпывающую договоренность Сторон и заменяет собой все предшествующие обсуждения, заверения, условия и договоренности по Положению.
   5. **Автономность положений**. Любое положение настоящего Положения, которое является запрещенным или не имеющим юридической силы, будет недействительным исключительно в объеме такого запрещения или отсутствия законной силы, не делая недействительными остальные положения настоящего Положения. Недействительное положение настоящего Положения должно быть заменено Сторонами новым положением, которое будет максимально схоже с недействительным с экономической точки зрения и с точки зрения целей настоящего Положения.
   6. **Разрешение споров**. В части разрешения споров Сторон, которые вытекают из данного Положения, применяются правила, установленные в Договоре.
   7. **Заключение Положения и переписка**. Положение может быть заключено путем обмена Сторонами по электронной почте экземплярами Положения, подписанными в одностороннем порядке. Стороны признают юридическую силу за документами, направленными по электронной почте, и признают их равнозначными документам на бумажных носителях, подписанным собственноручной подписью. Положение может быть также подписано с использованием сервисов электронной подписи (например, DocuSign). В случае использования сервисов электронной подписи подписант документа определяется в соответствии с правилами такого сервиса, в том числе по адресам электронной почты, которые указаны на странице с подписями настоящего Положения. Стороны обязуются не предоставлять доступ (в том числе пароли) к электронной почте и сервисам электронной подписи неуполномоченным лицам.

[*страница с подписями следует далее*]

\* \* \*

**ПОДПИСИ СТОРОН**

**Заказчик**  
[email]

Подпись: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *М.П.*

Дата: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ФИО: [ФИО]

Должность: [Должность]

**Исполнитель**  
[email]

Подпись: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *М.П.*

Дата: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ФИО: [ФИО]

Должность: [Должность]