Обязательные условия сотрудничества
для контрагентов Группы компаний «СберРешения»

Юридическое лицо или индивидуальный предприниматель (далее – Контрагент) вступившее в переговоры или заключившее договор с юридическим лицом, входящим в Группу компаний «СберРешения» (далее - СберРешения), Контрагент присоединяется к Обязательные условия сотрудничества (далее – ОУС).

1. Заверения об обстоятельствах

1.1. Стороны заверяют друг друга, что каждая из Сторон:
- 1.1.1. является юридическим лицом/индивидуальным предпринимателем, надлежащим образом учрежденным и правомерно осуществляющим свою деятельность в соответствии с законодательством РФ;
- 1.1.2. обладает полной дееспособностью на заключение Договора и исполнение всех своих обязательств, возникающих из Договора или в связи с ним;
- 1.1.3. получила все необходимые согласия на заключение и исполнение Договора;
- 1.1.4. располагает необходимыми ресурсами для исполнения своих обязательств.

1.2. Контрагент заверяет СберРешения, что на момент заключения Договора:
- 1.2.1. Участники и руководители Контрагента не имеют количественных и качественных критериев для признания их массовыми участниками и руководителями;
- 1.2.2. Исполнительный орган Контрагента находится и осуществляет функции управления по месту регистрации юридического лица;
- 1.2.3. В исполнительном органе Контрагента нет дисквалифицированных лиц;
- 1.2.4. Контрагент своевременно и в полном объёме уплачивает налоги, взносы и сборы и представляет отчётность, ведет бухгалтерский и налоговый учёт, не уклоняется от взаимодействия с контролирующими органами;
- 1.2.5. Контрагент не находится в процедуре несостоятельности (банкротства);
- 1.2.6. Контрагент отражает все финансово-хозяйственные операции;
- 1.2.7. Отсутствуют любые обстоятельства, способные повлиять на возможность Контрагента исполнять свои обязательства;
- 1.2.8. В случае проведения налоговой проверки СберРешений Контрагент передаст налоговым органам документы, которые будут истребованы в соответствии с действующим законодательством;
- 1.2.9. Информация, предоставленная Контрагентом, является достоверной, полной и точной.
- 1.2.10. Контрагент не скрыл никаких обстоятельств, которые при их обнаружении могли бы негативно повлиять на решение СберРешений заключить Договор.

1.3. При заключении и исполнении Договора СберРешения полагаются на достоверность, точность и полноту заверений об обстоятельствах Контрагента.

1.4. Если Контрагент предоставил недостоверные заверения об обстоятельствах, СберРешения вправе в одностороннем порядке отказаться от исполнения Договора путем направления уведомления.

1.5. Договор считается расторгнутым с даты, указанной в уведомлении, а если дата не указана - по истечении 5 рабочих дней с момента доставки уведомления.

2. Антикоррупционная оговорка

2.1. Стороны обязуются не осуществлять действий, квалифицируемых действующим законодательством РФ и нормами международного права как «коррупция».

2.2. Стороны, их работники, уполномоченные представители и посредники (далее – Представители) прямо или косвенно не оказывают влияние на действия или решения любых лиц с целью получения выгод или достижения иных целей, в том числе:
- Не обещают и не предлагают денег, ценных бумаг, иного имущества или имущественных прав, а также оказание услуг или выполнение работ (далее – Ценности);
- Не предоставляют и не разрешают предоставление Ценностей;
- Не требуют предоставление Ценностей.

2.3. Стороны и их Представители не осуществляют действия (бездействие), квалифицируемых действующим законодательством РФ и нормами международного права как:
- Дача или получение взятки;
- Коммерческий подкуп;
- Посредничество во взяточничестве или коммерческом подкупе;
- Злоупотребление полномочиями;
- Незаконное вознаграждение от имени юридического лица.

2.4. Стороны и их Представители обязуются:
- Уведомлять друг друга о обстоятельствах, которые являются или могут явиться основанием для возникновения конфликта интересов;
- Воздерживаться от совершения действий (бездействия), влекущих за собой возникновение или создающих угрозу возникновения конфликта интересов;
- Оказывать иное содействие друг другу в целях выявления, предупреждения и предотвращения коррупционных правонарушений и конфликтов интересов.

2.5. Сторона незамедлительно письменно уведомляет другую Сторону о сведениях, связанных с фактическим или возможным нарушением другой Стороной или его Представителем, антикоррупционных обязательств.
2.5.1. Уведомление Стороны должно содержать реквизиты Договора и описание фактических обстоятельств, связанных с антикоррупционных обязательств.
2.5.2. Сторона прикладывает к уведомлению доказательства нарушения.
2.6. Сторона, получившая уведомление, обеспечивает его конфиденциальное рассмотрение и предоставляет ответ в течение 30 календарных дней с даты получения уведомления.
2.7. В случае несогласия с фактическими обстоятельствами или доказательствами нарушения антикоррупционных обязательств, Сторона направляет мотивированные возражения и доказательства.
2.8. Сторона вправе отказаться от исполнения Договора в одностороннем порядке, путем направления уведомления, в случаях:
2.8.1. Получения от другой Стороны ответа, подтверждающего нарушение антикоррупционных обязательств;
2.8.2. Непредставления другой Стороной ответа на уведомление о нарушении антикоррупционных обязательств;
2.8.3. Непредставления другой Стороной мотивированных возражений и доказательств.
2.9. Договор считается расторгнутым с даты, указанной в уведомлении, а если дата не указана - по истечении 5 рабочих дней с момента его доставки.
2.10. Сторона, по инициативе которой был расторгнут Договор, вправе требовать возмещения реального ущерба, возникшего в результате такого расторжения.

3. Налоговая оговорка

3.1. Стороны заверяют друг друга, что:
3.1.1. Стороны соблюдают требования законодательства, в том числе в части:
- Надлежащего ведения налогового и бухгалтерского учёта;
- Полноты, точности и достоверности отражения операций в учёте;
- Исполнения налоговых обязательств по начислению и уплате налогов и сборов;
- Исполнения трудового законодательства и законодательства о социальном обеспечении;
- Полноты отражения в учете начислений и выплат работникам и уплачиваемых страховых взносов.

3.1.2. Основной целью совершения сделки и операций по Договору не являются неуплата налогов и/или зачет (возврат) суммы налогов.
3.2. Контрагент заверяет СберРешения, что в налоговых периодах, в течение которых совершаются операции по Договору:
3.2.1. Контрагент не осуществляет и не будет осуществлять уменьшение налоговой базы и/или суммы подлежащей уплате налога, страховых взносов в результате искажения сведений о фактах хозяйственной жизни (совокупности таких фактов), об объектах налогообложения и отчислений, в том числе за счет дробления бизнеса и/или необоснованного применения специальных налоговых режимов;
3.2.2. Все операции будут полностью отражены в первичных документах Контрагента и третьих лиц, привлеченных им в целях исполнения Договора, в обязательной бухгалтерской, налоговой, статистической и любой иной отчетности;
3.3. Контрагент возмещает имущественные потери СберРешений (ст. 406.1 ГК РФ), возникшие в случае:
- Невозможности уменьшения СберРешениями налоговой базы и/или суммы подлежащего уплате налога по операциям с Контрагентом и/или третьими лицами, привлеченными Контрагентом для исполнения Договора;
- предъявления налоговыми органами требований к СберРешениям об уплате налогов, сборов, страховых взносов, штрафов, пеней, а также отказа в возможности признать расходы для целей налогообложения прибыли или включить НДС в состав налоговых вычетов;
- предъявления третьими лицами требований о возмещении потерь и убытков в виде уплаченных ими налогов (пеней, штрафов), доначисленных налоговыми органами из-за отказа в применении налоговых вычетов по НДС и из-за исключения стоимости предмета Договора из расходов для целей налогообложения по причинам, связанным с действиями/бездействиями Контрагента.

3.4. Акт государственного органа будет являться достаточным доказательством возникновения и размера имущественных потерь, понесенных СберРешениями.
3.5. Факт оспаривания Акта государственного органа или претензий третьих лиц не влияет на обязанность Контрагента возместить имущественные потери, понесенные СберРешениями.

4. Конфиденциальность

4.1. Информация, полученная одной Стороной от другой в рамках Договора, является конфиденциальной.
4.2. Стороны обязаны защищать Конфиденциальную информацию, полученную от другой Стороны, как свою собственную.
4.3. Доступ к Конфиденциальной информации предоставляется только тем работникам и представителям Сторон, которые в силу своих должностных или договорных обязанностей, должны использовать Конфиденциальную информацию для достижения целей Договора.
4.4. При обработке Конфиденциальной информации не допускается:
- Разглашения Конфиденциальной информации третьим лицам;
- Использование Конфиденциальной информацию в целях, отличных от целей Договора;
- Осуществление копирования, записи, фото- и видеосъемки либо воспроизведение Конфиденциальной

информации, без согласия другой стороны.

4.5. Стороны обязаны за свой счёт возвратить или уничтожить полученную от другой Стороны Конфиденциальную информацию и её копии в течение 30 рабочих дней с даты получения письменного требования от другой Стороны.

4.6. Охрана и защита Конфиденциальной информации обеспечивается Сторонами в течение 3 лет с момента прекращения действия Договора.

Передача Конфиденциальной информации

4.7. Стороны заверяют друг друга, что имеют право на передачу Конфиденциальной информации другой Стороне.

4.8. Конфиденциальная информация может передаваться любым согласованным Сторонами способом.

4.9. Способ передачи должен исключать возможность несанкционированного доступа к Конфиденциальной информации и подтверждать факт её передачи и получения Сторонами.

4.10. Передача документов или материальных носителей, содержащих Конфиденциальную информацию, осуществляется по акту приема-передачи.

4.11. На документах или материальных носителях, содержащих Конфиденциальную информацию, должна размещаться отметка «Конфиденциально» или «Конфиденциальная информация».

4.12. При передаче Конфиденциальной информации по электронной почте или иным способом с использованием сети Интернет, раскрывающая Сторона должна заранее и наглядно известить принимающую сторону о конфиденциальном характере информации.

4.13. Электронное сообщение должно содержать опись передаваемой Конфиденциальной информации.

Раскрытие и Разглашение Конфиденциальной информации

4.14. Стороны вправе раскрывать Конфиденциальную информацию по требованию уполномоченных государственных органов или постановления суда (далее – Требование).

4.15. Сторона обязана уведомить другую Сторону о поступлении Требования.

4.16. Уведомление должно содержать информацию о содержании Требования и сроках предоставления информации.

4.17. Сторона обязана принять разумные меры для того, чтобы раскрытие Конфиденциальной информации было ограничено объёмом, необходимым для выполнения Требования.

4.18. Сторона уведомляет другую Сторону о факте исполнения Требования и раскрытия Конфиденциальной информации.

4.19. Стороны обязаны незамедлительно уведомлять друг друга о фактах разглашения Конфиденциальной информации.

4.20. Виновная Сторона обязана провести расследование факта разглашения Конфиденциальной информации.

4.21. За разглашение Конфиденциальной информации, Сторона обязуется возместить другой Стороне документально подтвержденный реальный ущерб, но не более 500 000 рублей.

5. Персональные данные

5.1. Контрагент обязан обрабатывать персональные данные, полученные от СберРешений, в соответствии с действующим законодательством РФ в области обработки персональных данных (далее – Законодательство о персональных данных).

5.2. Контрагент обязуется привлекать работников к обработке персональных данных только после подписания ими обязательства об обеспечении конфиденциальности персональных данных.

5.3. Контрагент обязуется не раскрывать персональные данные третьим лицам за исключением случаев, предусмотренных Законодательством о персональных данных.

5.4. Контрагент обязуется уведомить СберРешения о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных третьим лицам, не позднее 12 часов после обнаружения данного факта.

5.5. Если передача персональных данных осуществляется посредством взаимодействия с ИТ-инфраструктурой СберРешений, Контрагент принимает условия Положения о соблюдении требований кибербезопасности (Приложение №1 к ОУС).

6. Обстоятельства непреодолимой силы

6.1. Сторона, для которой возникли обстоятельства непреодолимой силы, обязана в течение 15 календарных дней с момента возникновения таких обстоятельств уведомить другую Сторону о невозможности исполнения обязательств по Договору.

6.2. Срок исполнения Сторонами обязательств по Договору переносится соразмерно времени действия обстоятельств непреодолимой силы и устранения их последствий, но не более чем на 60 дней.

6.3. Если обстоятельства непреодолимой силы продолжают действовать более 60 дней, любая из Сторон вправе отказаться от исполнения Договора, письменно уведомив другую Сторону за 3 дня до даты расторжения.

7. Юридически значимые сообщения

7.1. Электронная переписка, осуществляемая Сторонами в процессе исполнения Договора, имеет полную юридическую силу и принимается к исполнению Сторонами, если она осуществляется с адресов, указанных в Договоре.

7.2. Электронная переписка считается полученной адресатом в дату получения соответствующего электронного письма.

7.3. Стороны обязуются уведомлять друг друга об изменении своих адресов и иных данных не позднее 7 календарных дней с даты таких изменений.

8. Интеллектуальная собственность

8.1. Контрагент заверяет, что при исполнении Договора не будут нарушены интеллектуальные права третьих лиц.

8.2. Если в ходе исполнения Договора Контрагентом и/или привлеченными им третьими лицами будут созданы результаты интеллектуальной деятельности (далее – РИД), Контрагент отчуждает исключительные права на РИД СберРешениям в полном объёме путем подписания Акта приема-передачи или УПД.

8.3. Контрагент заверяет, что на момент отчуждения исключительных прав на созданный РИД, Контрагент является единственным правообладателем.

8.4. По запросу СберРешений, Контрагент предоставляет документальное подтверждение принадлежности Контрагенту исключительных прав на РИД.

8.5. Контрагент согласен, что СберРешения будет использовать РИД без указания его наименования (анонимное использование) и заверяет, что получил согласие на анонимное использование РИД от всех авторов.

8.6. Контрагент оказывает содействие в урегулировании претензий и/или исков третьих лиц, связанных с нарушением интеллектуальных прав на РИД, а также в полном объёме возмещает убытки СберРешений, связанные с такими претензиями и/или исками.

9. Решение споров

9.1. Стороны разрешают споры в досудебном порядке в течение 30 календарных дней с даты доставки претензии.

9.2. Споры Сторон подлежат разрешению в Арбитражном суде города Москвы.

10. Реклама

10.1. Настоящий раздел применяется только к Контрагентам, в рамках отношений с которыми используются рекламные материалы СберРешений и/или оказываются Услуги/выполняются Работы по размещению рекламных материалов СберРешений.

10.2. При использовании рекламных материалов СберРешений или их размещению Контрагент обязан:

10.2.1. Получать от СберРешений письменное согласие на публикацию любых рекламных материалов СберРешений до их публикации;

10.2.2. Согласовывать со СберРешениями любые рекламные материалы СберРешений и способ их распространения;

10.2.3. Использовать логотип и товарный знак СберРешений только с предварительного письменного согласия СберРешений.

10.3. Контрагент при размещении рекламных материалов СберРешений в сети Интернетобязуется соблюдать требования законодательства РФ о рекламе, в том числе:

- обеспечивать маркировку рекламных материалов СберРешений по форме: «Реклама. Рекламодатель АО «Интеркомп» или «Реклама. Сайт Рекламодателя: https://sber-solutions.ru/»;
- передавать информацию о рекламе СберРешений, публикуемой на ресурсах Контрагента или иным образом распространяемой силами Контрагента, в единый реестр интернет-рекламы Роскомнадзора (ЕРИР) своими силами или с привлечением оператора рекламных данных.

10.4. В случае публикации Контрагентом рекламных материалов о СберРешениях или внесения изменений в рекламные материалы без согласования со СберРешениями, СберРешения имеют право отказаться от Договора в одностороннем порядке без возмещения фактически понесенных Контрагентом расходов, требовать возврата суммы оплаченной стоимости Услуг/Работ соразмерно периоду до отказа от Договора, компенсации ущерба в полном объёме, а также уплаты штрафа в размере, предусмотренном Договором, в течение 10 дней с момента доставки требования СберРешения.

10.5. Контрагент в полном объёме возмещает убытки СберРешений, связанные с требованиями третьих лиц или государственных органов власти, связанными с неисполнением или ненадлежащим исполнением Контрагента обязательств по распространению рекламных материалов.

11. Изменение ОУС

11.1. СберРешения вправе изменять ОУС (далее – Изменения), путем опубликования их новой редакции на сайте СберРешений.

11.2. Изменения вступают в силу по истечении 5 рабочих дней с момента их размещения на сайте СберРешений.

11.3. Контрагент самостоятельно и регулярно проверяет Изменения на сайте СберРешений.

11.4. В случае несогласия Контрагента с Изменениями - Контрагент вправе отказаться от Договора.

11.5. Контрагент отказывается от Договора путём направления уведомления об отказе от Договора до вступления в силу Изменений.

11.6. Если Контрагент своевременно не направил уведомление - Изменения считаются принятыми Контрагентом.

12. Прочие положения

12.1. Стороны не несут ответственности за косвенные убытки и упущенную выгоду другой Стороны.

12.2. Контрагент не вправе распространять информацию о факте наличия договорных отношений с СберРешениями, без предварительного письменного согласия СберРешений.

12.3. Стороны вправе подписать Договор и иные документы к нему с использованием E-invoicing или иных систем электронного документооборота.
12.4. С даты заключения Договора вся предшествующая переписка, документы и договоренности Сторон по вопросам, являющимся предметом Договора, утрачивают силу.
12.5. В случае признания недействительным любого положения Договора, остальные положения Договора сохраняют свою юридическую силу.
12.6. Условия Договора имеет приоритет над ОУС.
12.7. ОУС вступают в силу с даты вступления в силу Договора и действуют в течение всего срока действия Договора.
12.8. Приложение: 1. Положение о соблюдении требований кибербезопасности.

Приложение № 1

к Обязательным условиям сотрудничества
для Контрагентов группы компаний «СберРешения»

Положение о соблюдении требований кибербезопасности

Положение о соблюдении требований кибербезопасности (далее – Положение) распространяется на отношения Сторон, связанные с исполнением обязательств, предусматривающих любое взаимодействие с ИТ-инфраструктурой СберРешений:

- Передачу данных СберРешений посредством взаимодействия с ИТ-инфраструктурой СберРешений;
- Подключение и предоставление доступа к ИТ-инфраструктуре СберРешений;
- Разработку ПО;
- Установку, настройку, модификацию, адаптацию, внедрение, техническую поддержку, сопровождение программного обеспечения (далее - ПО) и автоматизированных систем (далее - АС) в ИТ-инфраструктуре СберРешений;
- Использование облачного сервиса (SaaS, PaaS, IaaS).
- Иное взаимодействия в ИТ-инфраструктуре СберРешений.

1. Заверения об обстоятельствах

1.1. Контрагент заверяет, что заблаговременно обеспечит возможность надлежащего исполнения требований Положения.
1.2. Контрагент обязан ознакомить своих работников с Обязательством о соблюдении требований кибербезопасности работником контрагента (Приложение №1 к Положению), а работники Контрагента обязуются их соблюдать.
1.3. Контрагент привлекает третьих лиц к исполнению Договора только с письменного согласия СберРешений.
1.4. Контрагент несёт ответственность за действия и/или бездействия привлекаемых им третьих лиц.
1.5. Условия передачи и обработки Конфиденциальной информации СберРешений третьим лицом, привлеченным Контрагентом, определяются отдельным договором между СберРешениями и привлечённым третьим лицом.
1.6. СберРешения вправе осуществлять оценку Контрагента на соответствие требованиям Положения и Законодательства о персональных данных по внутренней методике (далее - Оценка).
1.7. Оценка может проводиться до заключения и в течение действия Договора, путем анкетирования.
1.8. Контрагент обязуются заполнить анкету и предоставить её СберРешениям в согласованный Сторонами срок.
1.9. Если результат Оценки будет «неудовлетворительный», СберРешения вправе прекратить переговоры о заключении Договора или в одностороннем порядке отказаться от исполнения Договора путем направления уведомления.
1.10. Договор считается расторгнутым с даты, указанной в уведомлении, а если дата не указана - по истечении 5 рабочих дней с момента его доставки.

2. Взаимодействие с ИТ-инфраструктурой

2.1. Контрагент обязан письменно согласовать подключение любого оборудования и ИТ-инфраструктуры к ИТ-инфраструктуре СберРешений.
2.2. Предоставление доступа Контрагенту и работнику Контрагента к ИТ-инфраструктуре СберРешений допускается только в целях исполнения обязательств по Договору и после проверки их на благонадежность.
2.3. При осуществлении технического обслуживания и поддержки оборудования/СВТ СберРешений, не подключённого к локальной вычислительной сети (далее – ЛВС) СберРешений, Контрагент обязан своевременно обновлять системное и прикладное ПО такого оборудования/СВТ СберРешений.
2.4. СВТ Контрагента, взаимодействующие со СберРешениями, размещаются в выделенных сетевых сегментах Контрагента, изолированных от сети Интернет, их взаимодействие с внутренней сетью Контрагента осуществляются только в рамках согласованной Сторонами схемы.
2.5. Запрещается информационное взаимодействие между Контрагентом и СберРешениями по сетевым протоколам без использования шифрования трафика.
2.6. Способ организации защищённого удалённого доступа к ИТ-инфраструктуре СберРешений, технические параметры подключения, тип и настройки оборудования, используемого для удалённого доступа, определяются СберРешениями.
2.7. Почтовый трафик между Контрагентом и СберРешениями должен передаваться внутри VPN-туннеля или с использованием шифрования. При использовании протокола TLS должна использоваться версия не ниже 1.2.
2.8. При организации VPN-туннеля между ИТ-инфраструктурами СберРешений и Контрагента должны выполняться требования:
    - подключение Контрагента к ИТ-инфраструктуре СберРешений осуществляется путем установки сетевого соединения СВТ Контрагента с СВТ внешней сети СберРешений с обязательной трансляцией IP-адресов на сетевом оборудовании Контрагента в диапазон адресов, выданный СберРешениями и закрепленный за Контрагентом. Защита соединения в этом случае реализуется с помощью средств криптографической защиты информации;
    - использование технологии remote access VPN допускается только для подключения Контрагента к инфраструктуре СберРешений с использованием виртуальных автоматизированных рабочих мест (далее – АРМ) СберРешений.
2.9. В случае, если Контрагент обрабатывает данные СберРешений в своей ИТ-инфраструктуре, он обязуется:
    - для сегмента ЛВС, содержащего АС, обрабатывающие данные СберРешений, обеспечивать соблюдение применимых к Контрагенту (как законодательно установленных, так и определяемых Договорами, в случае их наличия) требований к защите информации;

- уведомлять СберРешения перед внесением изменений в архитектуру ЛВС и средств обеспечения кибербезопасности (далее – КБ) в сегменте ЛВС, содержащем АС, обрабатывающие данные СберРешений в случае, если такие изменения могут снизить уровень безопасности данного сегмента ЛВС;
- уведомлять СберРешения о доработках АС, обрабатывающих данные СберРешений;
- по запросу СберРешений предоставлять доступ работникам СберРешений для демонстрации нового (измененного) функционала и после согласования устранять замечания, выявленные работниками СберРешений;
- обеспечивать обработку данных СберРешений на выделенных физических или виртуальных серверах, отдельно от данных других клиентов Контрагента. Технологию изоляции данных Контрагент обязан согласовать со СберРешениями;
- выделять АС, обрабатывающие данные СберРешений, и АРМ Контрагента, использующиеся для управления такими АС и информационными ресурсами, в отдельный сегмент ЛВС со строго ограниченным доступом. Указанный сегмент должен быть изолирован от прямого взаимодействия с сетью Интернет.

2.10. Контрагент обязуется самостоятельно или с привлечением третьих лиц обеспечить защиту своей ИТ-инфраструктуры, а также доменов, принадлежащих Контрагенту или СберРешениям и расположенных на внешних хостинг-площадках, от DDOS-атак техническими средствами. Пропускная способность полезного входящего траффика должна быть не менее 90 % на пике атаки.

Требования к сканированию защищённости и аудиту КБ при подключении АС-АС

2.11. Контрагент обязан не реже одного раза в квартал, проводить сканирование защищённости внешнего периметра ЛВС с привлечением внешних организаций, имеющих лицензии ФСТЭК на деятельность по технической защите Конфиденциальной информации.

2.12. Область сканирования защищённости должна включать, СВТ и сетевое оборудование:
- взаимодействующее с ИТ-инфраструктурой СберРешений;
- сетевой траффик с которыми разрешен для АС или СВТ, обрабатывающих данные клиентов СберРешений.

2.13. В случае выявления по результатам сканирования уязвимостей, эксплуатация которых потенциально несёт угрозу данным СберРешений, Контрагент обязан устранить данные уязвимости, а в случае невозможности устранения – незамедлительно уведомить СберРешения.

2.14. Контрагент обязан не реже одного раза в года, проводить внешние аудиты КБ.

2.15. Аудит должен проводится организацией, имеющей лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации.

2.16. Ежегодный аудит должен включать тестирование на проникновение из внутренней сети Контрагента, из сети Интернет и пентест веб-сервисов Контрагента.

2.17. По завершении аудита Контрагент обязуется предоставить СберРешениям отчёт и план устранения выявленных уязвимостей и недостатков, на согласование СберРешениям.

3. Использование облачного сервиса

3.1. Контрагент обязан соблюдать Требования к сканированию защищённости и аудиту КБ при подключении АС-АС.

3.2. Облачный сервис должен соответствовать стандартам управления информационной безопасности в облачных службах, предусматривающими реализацию организационных мер и использование современных технических (аппаратных и программных) средств, позволяющих определять актуальные угрозы и уязвимости КБ и надлежащим образом организовывать защиту информации СберРешений.

3.3. Все взаимодействия СберРешений с облачным сервисом должны осуществляться посредством защищённого соединения с использованием актуальных протоколов шифрования.

3.4. Почтовый трафик между Контрагентом и СберРешениями должен передаваться внутри VPN-туннеля или с использованием шифрования. При использовании протокола TLS должна использоваться версия не ниже 1.2.

3.5. Облачный сервис должен предоставлять возможность управления доступом на основе ролевой модели и ограничивать пользователям доступ к данным СберРешений.

3.6. Управление паролями в облачном сервисе при доступе к данным СберРешений должно осуществляться в соответствии со следующими требованиями:
- обязательная длина пароля должна быть не менее 12 символов;
- пароль должен содержать в себе: буквы верхнего и нижнего регистра, цифры и спецсимволы ($, #, % и т.д.);
- пароль не должен повторять предыдущие 5 паролей для данной учётной записи.

3.7. Должна быть предусмотрена возможность использования двухфакторной аутентификации для доступа к облачному сервису.

3.8. Данные СберРешений должны храниться в облачном сервисе в зашифрованном виде.

3.9. Контрагент обязан обеспечить резервное копирование данных СберРешений, размещенных в облачном сервисе, на нескольких географически распределенных площадках.

3.10. Контрагент обязан выполнять условия для обеспечения возможности проведения расследований инцидентов КБ.

3.11. Журналы аудита подлежат оперативному хранению в течение 6 месяцев и архивному в течение 1 года с условием соблюдения их доступности, целостности и конфиденциальности.

3.12. Журналы аудита должны передаваться по требованию СберРешений и содержать:

- события по загрузке и выгрузке информации (дата, время, название файла, хэш-сумма, ip-адрес, учётные данные);
- события авторизации (дата, время, ip-адрес, учётные данные);
- инциденты безопасности (дата, время, ip-адрес, тип события).

3.13. Контрагент обязан осуществлять содействие СберРешениям в предоставлении информации в рамках расследований инцидентов КБ, связанных с предоставлением услуг облачного сервиса.

3.14. Контрагент обязуется самостоятельно или с привлечением третьих лиц обеспечить защиту своей ИТ-инфраструктуры, а также доменов, принадлежащих Контрагенту или СберРешениям и расположенных на внешних хостинг-площадках, от DDOS-атак техническими средствами. Пропускная способность полезного входящего траффика должна быть не менее 90 % на пике атаки.

3.15. При расторжении Договора Контрагент обязан обеспечить возможность передачи данных СберРешениям и удалить их.

4. Разработка программного обеспечения

4.1. Контрагент несёт ответственность и заверяет, что исполнение Договора не приведет к появлению:

- в ПО СберРешений, ПО, используемого на условиях открытых лицензий (free and open-source software), условия которых требуют от пользователя раскрытия исходного кода, модифицированного ПО, либо ограничивают право пользователя запрещать третьим лицам использование модифицированного ПО. Под ПО СберРешений в рамках Положения понимается ПО, исключительное право на которое принадлежит СберРешениям на момент заключения Договора и/или возникает (переходит) у СберРешений в результате надлежащего исполнения Договора;
- скрытых функциональных возможностей и компьютерных вирусов, троянов, самоликвидирующихся механизмов, механизмов защиты от копирования и других подобных машинных команд, которые могут деактивировать, уничтожить или иным образом изменить данные СберРешений, программное или аппаратное обеспечение СберРешения.

4.2. Перед окончательной сдачей-приемкой ПО СберРешений, Контрагент обязан передавать его для проведения тестирования с участием специалистов СберРешений.

4.3. В целях проведения тестирования эталонный дистрибутив и исходные коды ПО передаются на хранение СберРешениям до проведения приемки.

4.4. Если в ходе тестирование обнаружены недостатки или несоответствие ПО условиям Договора, Контрагент устраняет недостатки в согласованный Сторонами срок и повторно предъявляет ПО на тестирование.

4.5. С исходных кодов на оборудовании СберРешений в присутствии Контрагента СберРешения вправе проводить контрольную компиляцию ПО.

4.6. СберРешения вправе требовать проведения процедуры депонирования исходных кодов, регулируемая отдельным соглашением СберРешений и Контрагента.

5. Информирование об инцидентах кибербезопасности

5.1. Контрагент обязан информировать СберРешения обо всех фактах нарушения требований Положения или событиях, способных привести к таким нарушениям.

5.2. Информирование осуществляется в максимально короткий срок, но не позднее 24 часов с момента обнаружения данного факта.

5.3. При возникновении в ИТ-инфраструктуре Контрагента значимого инцидента КБ, последствия которого могут привести к утрате целостности, доступности или конфиденциальности данных СберРешений, Контрагент обязан известить об этом СберРешения в максимально возможный короткий срок, но не позднее 3 часов с момента подозрения/обнаружения такого инцидента КБ.

5.4. Для повышения оперативности информация об инцидентах КБ передается в свободном формате и по любым каналам связи ответственным лицам СберРешения в рамках Договора и/или:

- по электронной почте: soc@sber-solutions.ru;
- по телефону: 8-495-660-13-77 (доб. 1727 или 3433).

5.5. Значимым считается инцидент КБ, удовлетворяющий по крайней мере один из следующих критериев:

- невозможность выполнения СберРешениями бизнес-операций, в соответствии с установленными сроками для структурного подразделения, или ограничение функциональности ИТ-услуги или АС;
- разглашение аутентификационных данных или конфиденциальной информации (в т.ч. персональные данные);
- воздействие вредоносного ПО, массовые блокировки учётных записей, создание несанкционированных учётных записей;
- выявленные признаки (в т.ч. неудачного получения) несанкционированного доступа, а также злоупотребление привилегиями.

5.6. В перечень инцидентов КБ Стороны включают инциденты, несущие риски потери конфиденциальности, целостности, доступности информации, в том числе:

- фишинговая атака от имени Стороны;
- эксплуатация выявленной уязвимости на ресурсе, принадлежащем Стороне;
- эксплуатация выявленной уязвимости в ПО, предоставляемом/эксплуатируемом Стороной;
- заражение вредоносным ПО;

- несанкционированный доступ к АС / информационным ресурсам;
- DDOS-атака на ресурсы Стороны – выявленная, закончившаяся или планируемая.

5.7. После устранения значимого инцидента КБ Контрагент обязан уведомить СберРешения о мерах, предпринятых для управления инцидентом, в срок не позднее 24 часов.

5.8. В рамках обмена информацией об инцидентах КБ Стороны не обмениваются информацией, содержащей персональные данные и иную информацию ограниченного доступа.

6. Заключительные положения

6.1. В случае нарушения Контрагентом требований Положения, СберРешения вправе отказать Контрагенту в предоставлении доступа к своей ИТ-инфраструктуре, а также отказаться от Договора в любое время без возмещения убытков Контрагенту, путем направления Контрагенту соответствующего уведомления не менее чем за 5 рабочих дней до момента расторжения Договора.

6.2. В каждом случае нарушения требований Положения, Контрагент выплачивает СберРешениям штрафную неустойку в размере 10 % от общего размера вознаграждения, и возмещает убытки СберРешений в полном объёме.

6.3. В случае предъявления СберРешениям требований со стороны третьих лиц, возникших в результате нарушения Контрагентом Положения, Контрагент обязан оказать СберРешениям содействие в урегулировании таких требований и возместить документально подтвержденные убытки в полном объёме.

6.4. СберРешения вправе в одностороннем порядке изменять условия Положения путем размещения новых условий Положения на сайте СберРешений.

6.5. Новые условия Положения применяются к отношениям Сторон с момент размещения их на сайте.

6.6. Контрагент обязан самостоятельно отслеживать изменения Положения.

6.7. Приложения: № 1. Обязательство о соблюдении требований кибербезопасности работником Контрагента.

Приложение № 1 к Положению

Обязательство о соблюдении требований кибербезопасности работником Контрагента

1. Нахождение на территории СберРешений

1.1. Не включать, не выключать и не работать с СВТ и АС СберРешений;

1.2. Не пытаться получить доступ к СВТ и АС СберРешений, за исключением общедоступных беспроводных сетей СберРешений.

1.3. Не оставлять без присмотра или передавать кому-либо пропуска, средства идентификации и ключи от помещений СберРешений.

1.4. Не производить самовольных отключений и подключений к локальной сети или СВТ СберРешений каких-либо носителей информации, личных устройств, беспроводных (радио) интерфейсов, модемов и прочего оборудования.

2. Работа с Конфиденциальной информацией

2.1. Если Работнику Контрагента предоставлен доступ к Конфиденциальной информации, Работник Контрагента обязан использовать её исключительно в целях исполнения обязательств по Договору.

2.2. Не разглашать и не использовать в личных целях и целях третьих лиц конфиденциальную информацию СберРешений, соблюдать конфиденциальность информации СберРешений.

2.3. Препятствовать ознакомлению посторонних лиц с конфиденциальными документами СберРешений, не допускать утрату (кражу, порчу, утерю) материальных носителей, содержащих Конфиденциальную информацию СберРешений.

2.4. Не хранить Конфиденциальную информацию СберРешений в общедоступных ресурсах, не передавать её за пределы сетей СберРешений в открытом виде, не использовать для передачи Конфиденциальной информации мессенджеры.

2.5. Без лишней необходимости не распечатывать электронные конфиденциальные документы СберРешений, забирать распечатанные документы из принтеров сразу после окончания печати и удалять файлы из папок сканирования.

2.6. По завершении использования уничтожать документы и медиа-носители, содержащие конфиденциальную информацию, методом механической переработки с помощью уничтожителей бумаг (шредеров).

2.7. Не разглашать и не распространять любую информацию СберРешений, полученную посредством любых средств коммуникации.

Электронные сообщения

2.8. Не открывать вложения и не переходить по ссылкам, указанным в почтовых сообщениях, имеющих признаки фишинга, включая:

- сообщение замаскировано под официальное письмо СберРешений и требует каких-либо быстрых действий или ответа;
- сообщение содержит ссылки на Интернет-ресурсы, визуально похожие на оригинальные ресурсы СберРешений, однако в отношении которых возникают сомнения;
- к сообщению прикреплен файл-вложение, который настойчиво предлагается открыть;
- в тексте сообщения содержатся опечатки, ошибки, избыточные знаки препинания.

2.9. Не переходить по коротким ссылкам.

2.10. Не рассылать с корпоративных почтовых адресов СберРешений сообщений развлекательного, рекламного и иного характера.

Пароли

2.11. Создавать пароль с соблюдением следующих требований:

- длина пароля должна быть не менее 12 символов;
- пароль должен содержать в себе: буквы верхнего и нижнего регистра, цифры, спецсимволы (например, $, #, %);
- пароль не должен совпадать с логином и повторять предыдущие 5 паролей для данной учётной записи;
- пароль не должен включать осмысленные слова, словосочетания, общепринятые аббревиатуры, а также основываться на доступных данных о пользователе или легко угадываемом алгоритме смены;
- пароль не должен содержать широко известные или легко угадываемые слова и последовательности символов;
- пароль по умолчанию должен быть изменён пользователем при первом входе;
- пароль должен изменяться не реже чем 1 раз в 30 дней с момента последнего изменения;
- в случае разглашения или компрометации пароль должен быть незамедлительно изменен.

2.12. Соблюдать правила обращения с паролями:

- не записывать пароль на предметах и материальных носителях, а также не хранить его в файле в открытом виде;
- не использовать один и тот же пароль для различных учётных записей;
- не передавать кому-либо свой пароль и не использовать чужие пароли для работы с СВТ и АС СберРешений;
- не осуществлять попытки подбора паролей, не пытаться завладеть паролями других лиц.

3. Работа с ИТ-Инфраструктурой СберРешений

3.1. При оставлении оборудования - блокировать его.

3.2. Не прерывать сканирование антивирусным ПО съёмных машинных и медиа носителей информации при их подключении к АРМ, включенному в сеть СберРешений.

3.3. Не организовывать на предоставленном компьютере ресурсы общего доступа и сетевые сервисы.

3.4. Не предпринимать попытки преодоления установленных СберРешениями ограничений, отключать и/или удалять установленные на предоставленных СВТ СберРешений средства защиты информации, использовать недокументированные свойства, ошибки в ПО и настройках защиты доступа к информационным ресурсам и АС СберРешений, доступ к которым не был предоставлен явным образом.

3.5. Не устанавливать на предоставленные СВТ СберРешений какое-либо ПО, изменять настройки уже имеющегося.

3.6. Не хранить и не использовать на предоставленном компьютере ПО результаты интеллектуальной деятельности в нарушение прав их законных правообладателей.

3.7. Не вскрывать корпус предоставленного компьютера (в том числе для самостоятельного устранения неисправностей), самовольно подключать к нему какое-либо оборудование (GPRS модемы, Wi-Fi точки доступа и пр.).

3.8. Не использовать без письменного согласования ПО следующих категорий при подключении к корпоративной сети СберРешений:

- сканеры портов и анализаторы трафика;
- средства для организации удалённого доступа, не утвержденные требованиями СберРешений, включая средства для создания зашифрованных каналов связи (VPN-, DNS-, SSH-, HTTPS-туннели и пр.);
- ПО, используемое для анонимного доступа в сеть Интернет (включая веб-сервисы, прокси-серверы);
- ПО для обхода средств защиты, включая средства подбора и восстановления паролей, поиска уязвимостей;
- ПО, предназначенное для сокрытия или внедрения дополнительной информации в цифровые объекты (в том числе реализующее методы стеганографии);
- ПО, осуществляющее сбор информации с клавиатуры, экрана, микрофона (снифферы);
- специализированные программные средства, оказывающее влияние на сетевые настройки СВТ, серверов и сетевого оборудования.

3.9. По требованию уполномоченных представителей СберРешений предоставлять выданные СВТ СберРешений и носители информации для проверки выполнения требований КБ.

3.10. Не использовать АРМ СберРешений (в том числе с использованием расширений к веб-браузеру) и личные СВТ, подключенные к сетям СберРешений, для посещения Интернет-ресурсов:

- содержание и направленность которых запрещены международным и российским законодательством;
- содержащих материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц;
- содержащих материалы, способствующие разжиганию межнациональной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия и т.д.

3.11. Информировать ответственное лицо СберРешений по вопросам КБ обо всех инцидентах КБ/обоснованных подозрениях на инцидент КБ и событиях, создающих угрозу причинения ущерба СберРешениям, а также об обращениях третьих лиц с целью незаконного получения конфиденциальной информации СберРешений.

4. Права СберРешений

4.1. Анализировать действия работника Контрагента при работе с АС СберРешений, оборудованием и СВТ, включая анализ отправленных информационных сообщений, в т.ч. с использованием корпоративных почтовых систем СберРешений и с использованием сети Интернет.

4.2. Использовать полученную в результате такого анализа информацию для проведения расследований, в т.ч., с привлечением правоохранительных органов, а также использовать в качестве доказательств в суде, в этих случаях Контрагент не вправе рассчитывать на соблюдение в отношении этих сообщений конфиденциальности со стороны СберРешений;

4.3. Приостановить доступ к своим АС, оборудованию, СВТ и в помещения СберРешений, в случае выявления нарушений.