СОГЛАШЕНИЕ
О КИБЕРБЕЗОПАСНОСТИ

Настоящее Соглашение о кибербезопасности (далее – Соглашение), является обязательным для юридических лиц имеющих или намеревающихся принять обязательства по договорам, приложениям/соглашениям, офертам, заключенным или заключаемым с Обществом с ограниченной ответственностью «Сбер2В» (ОГРН 1187746098583), именуемого в дальнейшем Общество.
Данное Соглашение является неотъемлемой частью Договора, содержащего ссылку на данный документ.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система – совокупность взаимосогласованных компонентов программного, технического, информационного, организационного, методического, правового обеспечения, используемая пользователями для реализации заданной информационной технологии.

Вредоносное программное обеспечение – программное обеспечение, предназначенное для получения несанкционированного доступа к устройству пользователя или к информации, хранимой на нем, с целью несанкционированного использования информационных ресурсов или причинения вреда.

Доступность – гарантия того, что авторизованные пользователи могут иметь доступ и работать с необходимыми информационными активами, ресурсами и системами с требуемой производительностью.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Общества, находящаяся в его распоряжении и представленная на любом материальном носителе в форме, пригодной для ее обработки, хранения или передачи.

Информационная инфраструктура Общества - совокупность информационных систем и подсистем, обеспечивающих функционирование и развитие информационного пространства Общества и средств информационного взаимодействия.

Информационный ресурс – отдельный документ или отдельный массив документов, документ или массив документов в автоматизированной системе (библиотеке, архиве, фонде, банке/базе данных и т.д.).

Информация Общества – любая информация, которая передается Обществом.

Инцидент кибербезопасности – реализованная угроза в киберпространстве, любое непредвиденное или нежелательное событие, которое может нарушить бизнес-процесс или состояние защищенности информационного актива.

Кибербезопасность – обеспечение защищенности Киберпространства, в котором функционирует бизнес, достигаемое применением набора средств, методик и принципов, направленных на противодействие Угрозам кибербезопасности и минимизацию последствий от их реализации. К задачам обеспечения кибербезопасности относится, в том числе, защита всех видов сведений конфиденциального характера, определенных в соответствии с применимым законодательством, включая, но не ограничиваясь персональными данными, сведениями, составляющими банковскую или коммерческую тайну, информацией об объектах критической информационной инфраструктуры. Под применимым законодательством понимается законодательство Российской Федерации, международные нормы и законодательство стран присутствия Общества, включая соответствующие нормативные правовые акты.

Киберпространство – информационное пространство, образованное совокупностью телекоммуникационных сетей и оборудования, средств вычислительной техники и программного обеспечения, а также деятельностью человека по его информационному наполнению.

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы,

избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Компания – юридическое лицо имеющее или намеревающееся принять обязательства по договорам, приложениям/соглашениям, офертам, заключенным с Обществом, предметом которого является предоставление удаленного доступа к ИТ-продуктам Общества, услуги по разработке, доработке (модификации, адаптации), настройке ПО и АС, оказываемые Обществу, по поддержке (сопровождению) ПО и АС, информационного и технологического взаимодействия и другие. .

Конфиденциальность – характеристика, определяющая, что информация не может быть доступной и раскрытой неавторизованным лицом, логическим объектом или процессом.

Конфиденциальная информация – информация, доступ к которой ограничен в соответствии с законом или по требованиям Общества с целью защиты прав и законных интересов субъектов права на тайну.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту Персональных данных).

Передача Персональных данных - взаимодействие, в рамках которого происходит передача Персональных данных от Общества Компании (включая предоставление и доступ).

Подключение – действие, последствием которого является передача информации между Оборудованием Компании и инфраструктурой или СВТ Общества.

Средства вычислительной техники – автоматизированные рабочие места и оргтехника (средства печати, копирования и сканирования и т.д.), а также серверное и сетевое оборудование.

Стороны – совместно именуемые по тексту настоящего Соглашения Общество и Компания.

Облачный сервис – информационная система общего пользования, построенная на основе облачного решения, предоставляющая функциональность обработки информации по одной из следующих моделей:

- «Программное обеспечение как услуга» (Software as a Service, SaaS) – пользователь удаленно использует прикладное программное обеспечение (далее – ПО), обслуживаемое Компанией;
- «Платформа как услуга» (Platform as a Service, PaaS) – пользователь использует информационно-технологические платформы, предоставляемые Компанией, включая системы управления базами данных и т.д., для размещения и удаленного использования своего прикладного ПО или информации;
- «Инфраструктура как услуга» (Infrastructure as a Service, IaaS) – пользователь использует вычислительные ресурсы (серверы, хранилища данных, сети), предоставляемые Компанией, для размещения и удаленного использования своего системного или прикладного ПО.

Оборудование – любые устройства, обладающие функционалом по обработке информации (включая ввод, хранение, отображение, поиск, передачу, коммутацию, управление), которые могут быть подключены к СВТ Общества по интерфейсам (включая беспроводные), предназначенным для передачи данных.

Объект защиты – элемент информационной инфраструктуры или набор элементов, объединенных определенным функциональным качеством (АРМ, сервер, АС, платформа, сетевое оборудование, сегмент сети, домен, группа доменов, ИТ-сервис и пр.).

Угроза кибербезопасности – совокупность условий и факторов, создающих потенциально или реально существующую опасность нарушения кибербезопасности в отношении Объекта зашиты.

Уязвимость – недостаток в компьютерной системе, использование которого приводит к нарушению целостности системы и некорректной работе.

Целостность – свойство сохранения правильности и полноты информационных активов Общества.

2. СОКРАЩЕНИЯ

DDOS Distributed Denial of Service

(атака типа «распределенный отказ в обслуживании»)

АС	Автоматизированная система
АРМ	Автоматизированное рабочее место
ВПО	Вредоносное программное обеспечение
ИР	Информационный ресурс
ИТ	Информационные технологии
КБ	Кибербезопасность
ЛВС	Локальная вычислительная сеть
НДВ	Недекларированная возможность
НПА	Нормативно-правовой акт
НСД	Несанкционированный доступ
ПО	Программное обеспечение
РФ	Российская Федерация
СВТ	Средства вычислительной техники
СОКБ	Система обеспечения кибербезопасности
СКЗИ	Средства криптографической защиты информации
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю

3. ПРЕДМЕТ СОГЛАШЕНИЯ

3.1. В соответствии с Соглашением Компания обязуется безоговорочно соблюдать требования по кибербезопасности, применять защитные меры и проводить мероприятия, перечисленные в разделах 4 и 5 Соглашения. Условия Соглашения являются обязательными для Компании и распространяются на отношения, связанные с исполнением обязательств, принятых по[1] договорам, приложениям/дополнительным соглашениям, офертам, заключенным с Обществом, включая, но не ограничиваясь, договорами поставки данных, договорами о предоставлении Компанией Обществу услуг по разработке, доработке (модификации, адаптации), настройке ПО и АС, по поддержке (сопровождению) ПО и АС, договорами информационного и технологического взаимодействия, договорами по предоставлению удаленного доступа к ИТ-продуктам Общества.

3.2. Обязательство Компании по исполнению требований по кибербезопасности, применению защитных мер, проведению мероприятий и иных условий, установленных Соглашением, является обстоятельством, имеющим существенное значение для Общества для заключения, исполнения и прекращения договоров, указанных в п. 3.1 Соглашения (по смыслу п. 2 ст. 431.2 Гражданского кодекса РФ).

4. ТРЕБОВАНИЯ ПО КИБЕРБЕЗОПАСНОСТИ

4.1. Условиями заключения Соглашения является наличие действующего соглашения о неразглашении конфиденциальной информации, заключенного по форме, предложенной Обществом. Стороны особо оговорили, что допускается одномоментное подписание соглашения о неразглашении конфиденциальной информации и договоров, указанных в п.3.1. настоящего Соглашения.

4.2. СВТ Компании, взаимодействующие с Обществом, должны быть размещены в выделенных сетевых сегментах Компании, изолированных от сети Интернет (кроме взаимодействий, минимально необходимых для оказания услуг Обществу), их взаимодействие с внутренней сетью Компании должно осуществляться только в рамках схемы взаимодействия, согласованной с Обществом.

4.3. При обработке данных Общества должны использоваться серверы,

[1] В случае, если Компания в ходе исполнения договоров, указанных в п.3.1 Соглашения, вправе привлекать третьих лиц с целью исполнения договора субподряда на оказание услуг Обществу, предусматривающего доступ субподрядчика Компании к информационной инфраструктуре Общества, доступ субподрядчика Компании к информационной инфраструктуре Общества предоставляется только с целью исполнения обязательств по договору субподряда во исполнение договора между Компанией и Обществом на оказание услуг Обществу, а также после заключения между субподрядчиком Компании и Обществом Соглашения о КБ, распространяющегося на договор субподряда во исполнение договора между Компанией и Обществом,.

расположенные на территории Российской Федерации.

4.4. Запрещается организация информационного взаимодействия между Компанией и Обществом по сетевым протоколам без использования шифрования трафика.

4.5. Способ организации защищенного удаленного доступа к информационным ресурсам Общества, технические параметры подключения, тип и настройки оборудования, используемого для удаленного доступа, определяются Обществом.

4.6. Почтовый трафик между Обществом и Компанией должен передаваться внутри VPN-туннеля или с использованием шифрования; при использовании протокола TLS должна использоваться версия не ниже 1.3;

4.7. При организации VPN-туннеля между информационными инфраструктурами Общества и Компании должны выполняться следующие требования:

1. В случае получения доступа к Информационной инфраструктуре Общества, Компания обязуется выполнять Правила предоставления доступа, установленные Обществом, в соответствии с Приложением 1 к Соглашению.

2. Подключение Компании к инфраструктуре Общества осуществляется путем установки сетевого соединения СВТ Компании с СВТ внешней сети Общества с обязательной трансляцией IP-адресов на сетевом оборудовании Компании в диапазон адресов, выданный Обществом и закрепленным за Компанией; защита соединения в этом случае реализуется с помощью СКЗИ;

3. Использование технологии remote access VPN допускается только для подключения Компании к инфраструктуре Общества.

4. В случае, если Компания обрабатывает данные клиентов или сотрудников Общества в своей информационной инфраструктуре, она обязуется:

- для сегмента ЛВС, содержащего АС, обрабатывающие данные клиентов и сотрудников Общества, обеспечивать соблюдение применимых к Компании (как законодательно установленных, так и определяемых иными договорами между Компанией и Обществом, в случае их наличия) требований к защите информации;
- в порядке, установленном разделом 7 Соглашения, уведомлять Общество перед внесением изменений в архитектуру ЛВС и средств обеспечения КБ в сегменте ЛВС, содержащем АС, обрабатывающие данные клиентов и сотрудников Общества в случае, если такие изменения могут снизить уровень безопасности данного сегмента ЛВС;
- по запросу Общества, в порядке, установленном разделом 7 Соглашения, уведомлять Общество о доработках АС, обрабатывающих данные клиентов и сотрудников Общества;
- по запросу Общества предоставлять доступ работникам Общества для демонстрации нового (измененного) функционала и после согласования устранить замечания, выявленные работниками Общества;
- обеспечить обработку данных клиентов Общества на выделенных физических или виртуальных серверах отдельно от данных других клиентов Компании; технологию изоляции данных Компания обязана согласовать с Обществом.
- выделить АС, обрабатывающие данные клиентов и сотрудников Общества, а также АРМ Компании, использующиеся для управления такими АС и ИР, в отдельный(е) сегмент(ы) ЛВС со строго ограниченным доступом (для АС и сотрудников Компании предоставляется минимальный доступ, достаточный для оказания услуг Обществу); указанный сегмент(ы) должен быть изолирован от прямого взаимодействия с сетью Интернет (кроме взаимодействий, минимально необходимых для оказания услуг Обществу).

4.8. Компания на постоянной основе, не реже одного раза в квартал, должна проводить сканирование защищенности внешнего периметра ЛВС, в том числе с привлечением внешних организаций, обладающих правом проведения таких работ на законном основании (наличие у такой организации лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации), при этом область сканирования должна включать, как минимум, СВТ и сетевое оборудование:

- взаимодействующее с инфраструктурой Общества;
- сетевой траффик с которыми разрешен для АС или СВТ, обрабатывающих данные клиентов или сотрудников Общества.

В случае выявления по результатам сканирования уязвимостей, эксплуатация которых потенциально несет угрозу данным клиентов или сотрудников Общества, Компания обязана в течение максимально короткого срока устранить данные уязвимости, а в случае невозможности устранения – незамедлительно информировать об этом Общество.

4.9. Компания обязуется на постоянной основе, не реже одного раза в год, проводить независимый аудит ИБ, внутренний аудит ИБ, а также проводить оценку соответствия требованиям по ИБ.

4.10. Компания обязуется самостоятельно или с привлечением внешней организации обеспечить защиту своей информационной инфраструктуры, а также доменов, принадлежащих Компании или Обществу и расположенных на внешних хостинг-площадках, от DDOS-атак. Защита должна быть организована с помощью применения технических средств и обеспечивать пропускную способность полезного входящего траффика не менее 90% на пике атаки.

5. ОБМЕН ИНФОРМАЦИЕЙ ОБ ИНЦИДЕНТАХ КИБЕРБЕЗОПАСНОСТИ

5.1. При возникновении в информационной инфраструктуре Компании или Общества значимого инцидента КБ, последствия которого могут привести к утрате целостности, доступности или конфиденциальности информации Общества, Компания обязана известить об этом Общество в максимально возможный короткий срок, но не позднее 3-х (трех) часов с момента обнаружения такого инцидента (подозрения на инцидент).

5.2. Компания должна заранее уведомлять о технических работах и иных запланированных работах, которые могут повлиять на доступность своих сервисов, и планируемых сроках их проведения.

5.3. Значимым считается инцидент КБ, удовлетворяющий одному из следующих критериев:

- ограничение функциональности ИТ-услуги или АС на срок больший, чем заявлено в уведомлении о проведении работ согласно п. 5.2 или предусмотрено соглашением об уровне услуг;
- повреждение или несанкционированное изменение информации, содержащейся в ИР и АС Общества, в том числе приводящее к невозможности использовать их;
- разглашение аутентификационных данных или конфиденциальной информации (коммерческая тайна, банковская тайна, персональные данные или иной конфиденциальной информации Общества);
- воздействие ВПО, массовые блокировки и несанкционированное создание учетных записей, затрагивающие сервисы, предоставляемые Обществу;
- выявленные признаки злоупотребления привилегиями, а также НСД или неудачного получения НСД, исключая отраженные средствами защиты информации.

5.4. В перечень инцидентов КБ включаются инциденты, несущие риски потери конфиденциальности, целостности, доступности данных, в том числе:

- фишинговая атака от имени Компании;
- эксплуатация выявленной уязвимости на ресурсе, принадлежащем Компании;
- эксплуатация выявленной уязвимости в ПО, предоставляемом/эксплуатируемом Компанией;
- заражение ВПО;
- НСД к АС / ИР, в том числе физический;
- DDOS-атака на Информационные ресурсы Компании.

5.5. В целях оперативного взаимодействия назначаются сотрудники, ответственные за обмен информацией о значимых инцидентах (подозрениях на инциденты) КБ, контакты ответственных лиц передаются путем направления письма на адреса электронной почтой указанные в договорах, указанных в п. 3.1 Соглашения.

5.6. В случае устранения значимого инцидента КБ Компания обязана не позднее 24 часов после устранения инцидента уведомить Общество о мерах, предпринятых для управления инцидентом.

5.7. Обмен информацией об инцидентах производится в свободном формате. Для повышения оперативности при передаче технической информации допускается использовать телефонную связь и иные каналы передачи информации, согласованные ответственными лицами.

5.8. В рамках обмена информацией об инцидентах КБ Стороны не обмениваются информацией, содержащей банковскую и государственную тайну, тайну связи, персональные данные и иную конфиденциальную информацию, кроме той, которая известна Сторонам в рамках выполнения работ по договору.

5.9. Если по условиям договора, заключаемого между Обществом и Компанией, осуществляется обмен конфиденциальной информацией, защита данных осуществляется в соответствии с разделом 4 Соглашения.

6. ПЕРСОНАЛЬНЫЕ ДАННЫЕ

6.1. Если по условиям договора, заключаемого между Обществом и Компанией, осуществляется обработка персональных данных, условия обработки и защиты таких данных должны определяться в соответствии с условиями такого договора или отдельного соглашения, посвященного обработке и защите персональных данных в рамках этого договора.

6.2. В случае, если по условиям договора, заключаемого между Обществом и Компанией, одна из Сторон осуществляет обработку персональных данных по поручению другой Стороны, в содержание соответствующего договора должно быть включено поручение на обработку персональных данных, либо Стороны должны заключить отдельный договор поручения обработки персональных данных

6.3. Общество и Компания принимают на себя обязательства обеспечить конфиденциальность и безопасность персональных данных, ставших им известными в ходе исполнения договоров, указанных в п. 3.1 настоящего Соглашения. Меры, принимаемые для обеспечения безопасности персональных данных и защиты прав субъектов персональных данных, должны соответствовать требованиям законодательства Российской Федерации.

6.4. При обработке персональных данных Общество и Компания обязуются принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных в соответствии с требованиями к защите обрабатываемых персональных данных, установленными статьей 19 Федерального закона № 152-ФЗ «О персональных данных» от 27.07.2006 г.

7. УВЕДОМЛЕНИЯ

7.1. Все уведомления, извещения и сообщения в связи с выполнением Соглашения, за исключением сообщений об инцидентах (раздел 5 Соглашения), должны быть оформлены в письменном виде на русском языке и могут быть направлены с помощью электронной почты, заказной или курьерской почтой, с подтверждением факта их получения, по адресу электронной почты, указанному в договорах, указанных в п. 3.1 Соглашения. В случае изменения адреса/реквизитов Компании, Компания обязана направить уведомление с актуальными данными на адрес электронной почты, указанный в договорах, указанных в п. 3.1 Соглашения, в течение 3 (трех) рабочих дней с момента изменения адреса/реквизита Компании.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Срок действия настоящего Соглашения равен сроку действия договору, указанному в п. 3.1 Соглашения.

8.2. Общество вправе изменять условия Соглашения по своей инициативе, без уведомления Компании о таких изменениях.

8.3. В течение действия Соглашения Общество вправе осуществлять контроль за соблюдением Компанией требований кибербезопасности. Данный контроль осуществляется Обществом путём направления в адрес Компании письменных запросов, ответ на которые Компания направить в адрес Общества в течение 10 рабочих дней с момента получения. Ответ направляется по электронной почте по адресу, указанному в договорах, указанных в п. 3.1 Соглашения.

8.4. Компания и Общество несут ответственность в соответствии с законодательством Российской Федерации. В случае нарушения Компанией принятых на себя обязательств по Соглашению, Компания обязуется возместить Обществу убытки, причиненные таким нарушением. Убытки возмещаются в соответствии с законодательством Российской Федерации. Кроме того, в случае, если к Обществу будут предъявлены претензии (требования, иски) со стороны третьих лиц или государственных органов, вследствие реализованных рисков КБ, в рамках Соглашения, Компания по получении извещения от Общества обязуется выступить на стороне Общества, оказать всемерное содействие Обществу при урегулировании таких претензий, в том числе взять на себя обязанность по подготовке и проведению досудебных переговоров и переписки с такими третьими лицами или государственными органами, а впоследствии (в том случае, если Общество будет вынуждено в силу вступившего в силу решения суда, или если по согласованию с Компанией будет признано приемлемым возместить ущерб третьих лиц во внесудебном порядке) возместить Обществу в полном объеме выплаченные Обществом третьим лицам или государственным органам денежные средства, все связанные с нарушением прав третьих лиц судебные издержки Общества и иные расходы. Возмещение производится Компанией не позднее 10 (десяти) рабочих дней со дня получения соответствующего требования от Общества.

8.5. Все споры, разногласия и требования, возникающие из Соглашения или в связи с ним, в том числе касающиеся его исполнения, нарушения, прекращения или недействительности, будут разрешаться сторонами претензионным путем. В случае если Компания или Общество посчитает, что ее право нарушено, она должна направить другой Стороне обоснованную претензию.

8.6. Компания или Общество, получившая претензию, обязана удовлетворить ее, либо направить мотивированные возражения в срок не более 10 (десяти) рабочих дней с момента получения претензии.

8.7. В случае, если претензия не удовлетворена и мотивированные возражения не получены, либо полученные мотивированные возражения не считаются обоснованными, споры подлежат разрешению в Арбитражном суде г. Москвы, применимое право – право Российской Федерации.

8.8. Не допускается передавать или иным образом уступать, полностью или частично, свои права и обязанности по данному Соглашению без предварительного письменного согласия на это Обществом.

Приложение 1 к Соглашению о кибербезопасности

Правила предоставления доступа к информационной инфраструктуре Общества (далее – Правила)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Общество предоставляет Компании доступ к информационным активам Общества, в том числе к ИТ-инфраструктуре и информационным системам, а Компания обязуется пользоваться доступом на условиях, предусмотренных настоящими Правилами.

1.2. Общество предоставляет Компании доступы к информационным активам только для целей исполнения обязанностей Компании в рамках Договора между Обществом и Компанией. Компания обязуется использовать предоставленные доступы исключительно в интересах Общества в случаях, указанных в пп.1. п.4.7. Соглашения.

1.3. Доступы предоставляются Компании на время исполнения обязанностей по Договору.

1.4. Компания обязуется до начала исполнения обязательств по Договору ознакомить с настоящими Правилами всех своих работников и, если применимо, привлекаемых для исполнения Договора третьих лиц, и обеспечить соблюдение ими настоящих Правил.

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. Общество обязано:

2.1.1. обеспечить предоставление доступа Компании к информационным активам Общества в целях исполнения обязанностей по Договору на условиях настоящих Правил.

2.2. Общество имеет право:

2.2.1. осуществлять контроль за использованием Компанией предоставленных доступов к информационным активам Общества;

2.2.2. в любой момент приостановить, ограничить и полностью закрыть доступ Компании к информационным активам Общества, в том числе в случае нарушения настоящих Правил со стороны работников Компании. При этом Общества направляет Компании соответствующее письменное уведомление в течение 3 (трех) рабочих дней с момента приостановления / ограничения / прекращения доступа к информационным активам. Приостановление доступа Компании к информационным активам в случае нарушения настоящих Требований не является основанием для освобождения Компании от ответственности за нарушение обязательств по Договору.

2.3. Компания обязана:

2.3.1. предоставить необходимую информацию по запросу Общества, в том числе перечень лиц Компании, которые будут уполномочены подавать заявки на первичное предоставление

(продление) доступа к информационным активам Общества для целей исполнения обязательств по Договору;

2.3.2. соблюдать положения настоящих Требований;

2.3.3. осуществлять замену своих работников, имеющих доступ к информационным активам Общества, на иных, только по письменному согласованию с Обществом, с обоснованием причин замены;

2.3.4. извещать Общество не менее чем за 5 (пять) рабочих дней до даты увольнения работника Компании или его отстранения от осуществления действий, связанных с использованием обязательств по Договору;

2.3.5. предоставлять Обществу возможность осуществлять контроль над работой Компании с предоставленными доступами к информационным активам Общества;

2.3.6. в случае попадания к работникам Компании паролей доступа, прав, полномочий и привилегий (умышленного или случайного), отличных от согласованных и выданных Обществом, Компания не вправе их использовать и обязана незамедлительно сообщить Обществу об их получении;

2.3.7. использовать предоставленные доступы, в том числе программное обеспечение, только для исполнения Компанией обязательств по Договору, в том числе не копировать, не воспроизводить программное обеспечение, не вносить в него изменения, не производить его анализ или декомпиляцию.

2.3.8. обеспечить конфиденциальность сведений, в том числе персональных данных, к которым был предоставлен доступ.

3. ПРЕДОСТАВЛЕНИЕ, ИЗМЕНЕНИЕ И ПРЕКРАЩЕНИЕ ПОЛНОМОЧИЙ ДОСТУПА

3.1. Первичное предоставление доступа работнику Компании к информационным активам Общества (создание учётной записи) предоставляется на основании официального письма Компании.

3.2. Обращения Компании по предоставлению или изменению доступа для работников Компании должны согласовываться уполномоченными работниками Общества, являющимися инициаторами основного Договора, в целях исполнения которого запрашиваются доступы, и далее обрабатываться в соответствии с установленными в Обществе процедурами.

3.3. В информационных активах Общества обрабатываются различные категории персональных данных. В случае предоставления доступа работникам Компании к информационным системам, обрабатывающим персональные данные, Компания обязуется выполнять требования законодательства Российской федерации в области защиты персональных данных.

3.4. После предоставления первичного доступа работнику Компании, последующие обращения на предоставления каких-либо доступов направляются работником Компании

самостоятельно и обрабатываются в соответствии с установленными в Обществе процедурами.

3.5. Обращения по предоставлению, изменению и блокировке доступа должны быть согласованы Обществом. При рассмотрении обращений уполномоченные работники Общества имеют право запросить и получить любую необходимую информацию по обращению, а также отклонить обращение без обоснования причин.

3.6. Общество имеет право в любой момент ограничить либо заблокировать доступ как отдельным работникам Компании, так и всем работникам Компании.

4. ТРЕБОВАНИЯ ПО СОБЛЮДЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Компании запрещается:

4.1.1. передавать другим лицам или разглашать в любой форме персональные атрибуты доступа к информационным активам, кроме своих работников, которым указанные персональные доступы будут предоставлены в целях исполнения обязательств по Договору;

4.1.2. самостоятельно подключать, отключать и вносить изменения в конфигурацию оборудования и информационных систем независимо от вида и назначения, если Договором прямо не предусмотрены подобные действия;

4.1.3. преднамеренно записывать, создавать, компилировать, копировать, распространять, запускать на выполнение или пытаться встраивать любые машинные коды, разработанные для само воспроизводства, повреждения или создания любых других помех функционированию информационных активов Общества, и нормальной работе других лиц;

4.1.4. самостоятельно устанавливать, загружать любые виды программного обеспечения на персональных компьютерах, принадлежащих Обществу;

4.1.5. размещать и хранить информацию, не имеющую отношения к обязанностям Компании по Договору (личную и развлекательного характера, в том числе фильмы, видеоклипы, музыку, игры, личные фотографии) на сетевых ресурсах, жестких дисках персональных компьютеров и других информационных активах Общества;

4.1.6. размещать и хранить информацию, имеющую отношение к обязанностям Компании по Договору, а также конфиденциальную информацию на локальных жестких дисках персональных компьютеров, не принадлежащих Обществу

4.1.7. осуществлять неправомерный доступ к охраняемой законом компьютерной информации, если это деяние может повлечь уничтожение, блокирование, модификацию либо копирование компьютерной информации;

4.1.8. устанавливать, использовать любые программные или аппаратные средства, позволяющие обезличивать, скрывать действия работников Компании;

4.1.9. устанавливать, использовать любые средства удаленного доступа или управления;

4.1.10. создавать дополнительные каналы выхода в сеть Интернет (к примеру, устанавливать внешние модемы), предпринимать попытки получить доступ в Интернет в обход настроек

действующей инфраструктуры и установленных Обществом правил использования доступа в Интернет;

4.1.11. самостоятельно изменять настройки операционной системы, установленной на компьютерном оборудовании.

5. ТРЕБОВАНИЯ ПО ПРИМЕНЕНИЮ ПАРОЛЕЙ

5.1. Все выбираемые работниками Компании пароли доступа к информационным активам Общества должны отвечать приведенным ниже требованиям:

- содержать не менее 12 символов для пользовательских паролей, не менее 16 символов для административных паролей;
- содержать: буквы различных регистров, цифры, спецсимволы;
- не являться словом из словаря, сленга, диалекта, жаргона;
- не являться личной информацией (к примеру, для создания паролей не должны применяться имена членов семьи, адреса, телефоны, даты рождения);
- не состоять из последовательностей символов раскладок клавиатуры (к примеру, 123456qwerty, 1qaz2wsx3456).

5.2. Пароли для доступа к информационным активам ограничиваться сроком действия договора, но не более 3-х месяцев единовременно, после чего подлежат продлению при необходимости путем повторного направления официального письма / запроса о продлении в срок, не превышающий 60 дней с момента истечения срока действия пароля.

5.3. Работники Компании обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей.

5.4. Запрещается:

- сообщать или разглашать свой пароль кому-либо, включая коллег, руководителей и работников службы технической поддержки, любыми средствами и способами;
- записывать, хранить пароли учетных записей пользователей в доступной для чтения форме в любом виде;
- использовать автоматическое сохранение пароля;
- использовать общие пароли доступа к персональным компьютерам совместно с другими работниками.

5.5. Пароль должен быть немедленно изменен, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого работника Компании.

5.6. Все текущие операции с паролем работники Компании должны осуществлять лично, не допуская возможности рассмотреть состав вводимого пароля и порядок введения символов.

5.7. Работникам Компании запрещается предпринимать какие-либо действия по получению (раскрытию) паролей не принадлежащих им учетных записей.

6. ТРЕБОВАНИЯ ПО АНТИВИРУСНОЙ БЕЗОПАСНОСТИ

6.1. Работникам Компании запрещается:

- деинсталляция или деактивация антивирусного ПО, а также изменение его настроек на персональных компьютерах Общества;
- создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

7. ОТВЕТСТВЕННОСТЬ КОМПАНИИ И ВОЗМЕЩЕНИЕ ПОТЕРЬ

7.1. При обнаружении фактов нарушения настоящих Требований, уполномоченный работник Общества уведомляет Компанию о факте нарушения и имеет право требовать объяснения. В случае не предоставления объяснений Компании в течение 3 (трех) дней с момента сообщения о факте нарушения без уважительной причины, все предоставленные Компании доступы к информационным активам Общества отзываются.