СОГЛАШЕНИЕ
О КИБЕРБЕЗОПАСНОСТИ

Настоящее Соглашение о кибербезопасности (далее – «Соглашение») является неотъемлемой частью договора, содержащего ссылку на Соглашение, заключенного между ООО «ДелоТех» ИНН 9725071534 (далее – «Общество») и его контрагентом (далее – «Контрагент», при совместном упоминании – «Стороны»).

1. ПРЕДМЕТ СОГЛАШЕНИЯ И ОБЩИЕ УСЛОВИЯ

1.1. Контрагент при исполнении обязательств по договору, содержащему ссылку на Соглашение (далее – Договор), обязуется соблюдать требования по кибербезопасности, применять защитные меры и проводить мероприятия, соблюдать иные условия, перечисленные в Соглашении.

1.2. Соблюдение Контрагентом условий Соглашения является обстоятельством, имеющим существенное значение для Общества в целях заключения, исполнения и прекращения Договора (по смыслу п. 2 ст. 431.2 ГК РФ).

1.3. Если Контрагент вправе привлекать третьих лиц для исполнения обязательств по Договору, в случае такого привлечения Контрагент обеспечивает исполнение третьим лицом условий Соглашения, как если бы оно выступали Контрагентом.

1.4. Если условия Договора противоречат условиям Соглашения, в части противоречия применяются условия Договора.

2. СОКРАЩЕНИЯ

АС	Автоматизированная система.
АРМ	Автоматизированное рабочее место
ИР	Информационный ресурс
КБ	Кибербезопасность
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
СВТ	Средства вычислительной техники
СКЗИ	Средства криптографической защиты информации
DDOS	Distributed Denial of Service, атака типа «распределенный отказ в обслуживании

3. 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.

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, полученная со стороны Общества или передаваемая 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.

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.

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

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

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.

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

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

Целостность – свойство сохранения правильности и полноты информационных активов Общества.

4. ТРЕБОВАНИЯ ПО КИБЕРБЕЗОПАСНОСТИ

4.1. СВТ Контрагента, взаимодействующие с Обществом, должны быть размещены в выделенных сетевых сегментах Контрагента, изолированных от сети Интернет (кроме взаимодействий, минимально необходимых для исполнения обязательств по Договору), их взаимодействие с внутренней сетью Контрагента должно осуществляться только в рамках схемы взаимодействия, согласованной с Обществом.

4.2. Обработка данных Общества допускается исключительно на серверах, расположенных на территории РФ.

4.3. Запрещается организация информационного взаимодействия между Контрагентом и Обществом по сетевым протоколам без использования шифрования трафика.

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

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

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

4.6.1. В случае получения доступа к Информационной инфраструктуре Общества Контрагент обязуется выполнять Правила предоставления доступа, установленные Обществом, в соответствии с Приложением к Соглашению, и требования локальных нормативных актов Общества, доведенных до Контрагента;

4.6.2. Подключение Контрагента к инфраструктуре Общества осуществляется путем установки сетевого соединения СВТ Контрагента с СВТ внешней сети Общества с обязательной трансляцией IP-адресов на сетевом оборудовании Контрагента в диапазон адресов, выданный Обществом и закрепленным за Контрагентом; защита соединения в этом случае реализуется с помощью средств криптографической защиты информации;

4.6.3. Использование технологии remote access VPN допускается только для подключения Контрагента к инфраструктуре Общества;

4.6.4. В случае, если Контрагент обрабатывает данные клиентов или сотрудников Общества в своей информационной инфраструктуре, он обязуется:

- для сегмента ЛВС, содержащего АС, обрабатывающие данные клиентов и сотрудников Общества, обеспечивать соблюдение применимых к Контрагенту требований к защите информации;
- в порядке, установленном разделом 6 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 6 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 Контрагента; технологию изоляции данных Контрагент обязана согласовать с Обществом.
- выделить АС, обрабатывающие данные клиентов и сотрудников Общества, а также АРМ Контрагента, использующиеся для управления такими АС и ИР, в отдельный(е) сегмент(ы) ЛВС со строго ограниченным доступом (для АС и сотрудников Контрагента предоставляется минимальный доступ, достаточный для исполнения обязательств по Договору); указанный сегмент(ы) должен быть изолирован от прямого взаимодействия с сетью Интернет (кроме взаимодействий, минимально необходимых для исполнения обязательств по Договору).

4.7. Контрагент на постоянной основе, не реже одного раза в квартал, должен 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 России 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, Контрагент обязан в течение максимально короткого срока устранить данные уязвимости, а в случае невозможности устранения – незамедлительно информировать об этом Общество.

4.8. Контрагент 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.

4.9. Контрагент обязуется самостоятельно или с привлечением внешней организации обеспечить защиту своей информационной инфраструктуры, а также доменов, принадлежащих Контрагенту 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.

4.10. В случае обработки персональных данных друг друга Стороны обязуются обеспечить принятие всех необходимых правовых, организационных и технических мер для защиты от неправомерных действий в отношении таких персональных данных в соответствии с требованиями законодательства РФ.

5. ОБМЕН ИНФОРМАЦИЕЙ ОБ ИНЦИДЕНТАХ КИБЕРБЕЗОПАСНОСТИ

5.1. При возникновении в информационной инфраструктуре Контрагента или Общества значимого инцидента КБ, последствия которого могут привести к утрате целостности, доступности или конфиденциальности информации Общества, Контрагент обязан 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. Контрагент должен 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, предусмотренной Договором или АС на срок больший, чем заявлено в уведомлении о проведении работ согласно п. 5.2 или предусмотрено Договором;
- 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 вредоносного программного обеспечения, 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 Контрагента;
- эксплуатация выявленной уязвимости на ресурсе, принадлежащем Контрагенту;
- эксплуатация выявленной уязвимости в ПО, предоставляемом / эксплуатируемом Контрагентом;
- заражение вредоносным программным обеспечением;
- НСД к АС / ИР, в том числе физический;
- DDOS-атака на информационные ресурсы Контрагента.

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 эл. почты, указанные в Договорах.

5.6. В случае устранения значимого инцидента КБ Контрагент обязан 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 (при условии последующего дублирования информации по эл. адресам ответственных лиц в течение 24 часов).

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 исполнения Договора.

5.9. Если по условиям Договора осуществляется обмен конфиденциальной информацией, защита данных осуществляется в соответствии с разделом 4 Соглашения.

6. УВЕДОМЛЕНИЯ

6.1. 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 адресам, указанным в Договоре.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Соглашение действует в течение срока действия Договора.

7.2. Общество вправе изменять условия Соглашения по своей инициативе путем размещения Соглашения на сайте в сети Интернет, без уведомления Контрагента о таких изменениях.

7.3. В течение действия Соглашения Общество вправе осуществлять контроль за соблюдением Контрагентом требований кибербезопасности. Данный контроль осуществляется Обществом путём направления в адрес Контрагента письменных запросов, ответ на которые Контрагент обязуется направить в адрес Общества в течение 10 рабочих дней с момента получения. Ответ направляется по электронной почте по адресу, указанному в Договоре.

7.4. Контрагент и Общество несут ответственность в соответствии с законодательством Российской Федерации. В случае нарушения Контрагентом принятых на себя обязательств по Соглашению, Контрагент 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, Контрагент 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 Контрагентом 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 Контрагентом не позднее 10 (десяти) рабочих дней со дня получения соответствующего требования от Общества.

7.5. Приложение к Соглашению является его неотъемлемой частью.

Приложение к Соглашению о кибербезопасности

ПРАВИЛА ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ

1. ОБЩИЕ ОБЯЗАННОСТИ КОНТРАГЕНТА

1.1. В рамках предоставления доступа к информационной инфраструктуре Общества Контрагент обязуется:

- до предоставления доступа ознакомить с настоящими Правилами всех работников и, если применимо, привлекаемых для исполнения Договора третьих лиц, участвующих в получении или реализации доступа к информационной инфраструктуре Общества, и обеспечить соблюдение ими настоящих Правил;
- предоставить необходимую информацию по запросу Общества, в том числе перечень лиц Контрагента, которые будут уполномочены подавать заявки на первичное предоставление (продление) доступа к информационным активам Общества для целей исполнения обязательств по Договору;
- осуществлять замену своих работников, имеющих доступ к информационным активам Общества, на иных, только по письменному согласованию с Обществом, с обоснованием причин замены;
- извещать Общество не менее чем за 5 (пять) рабочих дней до даты увольнения работника Контрагента или его отстранения от осуществления действий, связанных с использованием обязательств по Договору;
- предоставлять Обществу возможность осуществлять контроль над работой Контрагента с предоставленными доступами к информационным активам Общества;
- в случае попадания к работникам Контрагента паролей доступа, прав, полномочий и привилегий (умышленного или случайного), отличных от согласованных и выданных Обществом, Контрагент не вправе их использовать и обязан незамедлительно сообщить Обществу об их получении;
- использовать предоставленные доступы, в том числе программное обеспечение, только для исполнения Контрагентом обязательств по Договору, в том числе не копировать, не воспроизводить программное обеспечение, не вносить в него изменения, не производить его анализ или декомпиляцию.
- обеспечить конфиденциальность сведений, в том числе персональных данных, к которым был предоставлен доступ.

2. ПРЕДОСТАВЛЕНИЕ, ИЗМЕНЕНИЕ И ПРЕКРАЩЕНИЕ ДОСТУПА

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

2.2. Обращения Контрагента по предоставлению или изменению доступа для работников Контрагента обрабатываются в соответствии с локальными нормативными актами Общества.

2.3. В случае предоставления доступа работникам Контрагента к информационным системам, обрабатывающим персональные данные, Контрагент обязуется выполнять требования законодательства РФ в области защиты персональных данных.

2.4. После предоставления первичного доступа работнику Контрагента последующие обращения на предоставления каких-либо доступов могут быть направлены таким работником Контрагента самостоятельно и обрабатываются в соответствии с установленными в Обществе процедурами.

2.5. Общество вправе в любой момент приостановить, ограничить и полностью закрыть доступ Контрагента к информационным активам Общества, в том числе в случае нарушения настоящих Правил со стороны работников Контрагента. При этом Общество направляет Контрагенту соответствующее письменное уведомление в течение 3 (трех) рабочих дней с момента приостановления / ограничения / прекращения доступа к информационным активам.

2.6. При рассмотрении обращений уполномоченные работники Общества имеют право запросить и получить любую необходимую информацию по обращению, а также отклонить обращение без обоснования причин.

3. ТРЕБОВАНИЯ ПО СОБЛЮДЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Контрагенту запрещается:

- 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;
- самостоятельно подключать, отключать и вносить изменения в конфигурацию оборудования и информационных систем независимо от вида и назначения, если Договором прямо не предусмотрены подобные действия;
- преднамеренно записывать, создавать, компилировать, копировать, распространять, запускать на выполнение или пытаться встраивать любые машинные коды, разработанные для самовоспроизводства, повреждения или создания любых других помех функционированию информационных активов Общества, и нормальной работе других лиц;
- самостоятельно устанавливать, загружать любые виды программного обеспечения на персональных компьютерах, принадлежащих Обществу;
- размещать и хранить информацию, не имеющую отношения к обязанностям Контрагента 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;
- размещать и хранить информацию, имеющую отношение к обязанностям Контрагента по Договору, а также конфиденциальную информацию на локальных жестких дисках персональных компьютеров, не принадлежащих Обществу;
- осуществлять неправомерный доступ к охраняемой законом компьютерной информации, если это деяние может повлечь уничтожение, блокирование, модификацию либо копирование компьютерной информации;
- устанавливать, использовать любые программные или аппаратные средства, позволяющие обезличивать, скрывать действия работников Контрагента;
- устанавливать, использовать любые средства удаленного доступа или управления;
- 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;
- самостоятельно изменять настройки операционной системы, установленной на компьютерном оборудовании.

4. ТРЕБОВАНИЯ ПО ПРИМЕНЕНИЮ ПАРОЛЕЙ

4.1. Все выбираемые работниками Контрагента 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;
- не состоять из последовательностей символов раскладок клавиатуры (к примеру, qwerty123456).

4.2. Пароли для доступа к информационным активам ограничиваются 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.

4.3. Работники Контрагента обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей.

4.4. 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.
- Пароль должен быть немедленно изменен, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого работника Контрагента.

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

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

5. ТРЕБОВАНИЯ ПО АНТИВИРУСНОЙ БЕЗОПАСНОСТИ

5.1. Работникам Контрагента 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.