Соглашение о соблюдении требований информационной безопасности группы компаний Шлюмберже

Для целей настоящего Соглашения:
«Заказчик» означает Клиента (Шлюмберже, Заказчика, Покупателя, Арендатора) по настоящему Договору;
«Исполнитель» означает Экспедитора (Поставщика, Продавца, Подрядчика, Исполнителя, Арендодателя), по настоящему Договору.

Определения настоящего Положения

«Данные Заказчика» означает любую или всю информацию и материалы, полученные от любого лица/ представителя Компании, входящей в группу компаний Шлюмберже в России или хранящиеся в Информационных системах Заказчика.
«Исполнитель» - сторона, исполняющая обязанности по Договору (подрядчик/поставщик).
«Заказчик» - лицо/ представитель Компании, входящей в группу компаний Шлюмберже в России.
«**Субподрядчик**»- третье лицо, привлекаемое Исполнителем для выполнения части услуг по договору.
«Конфиденциальные данные» - Данные Заказчика, вся информация, сведения, полученные Стороной («Получающая Сторона») от другой Стороны («Раскрывающая Сторона») в ходе выполнения настоящего Договора, на которую распространяется юридическое преимущественное право.
«Нарушение безопасности» включает, но не ограничиваясь любыми из следующих категорий:

- несанкционированный доступ или несанкционированное использование Систем Исполнителя, в которых хранятся, обрабатываются или передаются Данные Заказчика;
- несанкционированный доступ или кража Данных Заказчика;
- несанкционированное использование Данных Заказчика лицом, имеющим санкционированный доступ к таким Данным в целях фактической или обоснованно подозреваемой кражи, мошенничества или кражи личных данных;
- несанкционированное раскрытие или изменение Данных Заказчика;

1. Общие положения

- Исполнитель обязан соблюдать требования настоящего приложения при оказании услуг Заказчику.
- Исполнитель не имеет права приостанавливать предоставление услуг Заказчику в одностороннем порядке. Исполнитель обязан направить уведомление о приостановке услуг не менее, чем за 30 календарных дней, если больший срок не согласован Договором/Заказом.
- Заказчик имеет право отстранить Исполнителя от работ, приостановить доступ к своим Информационным системам, оборудованию, средствам вычислительной техники и в помещения Заказчика, а в случае подтверждения факта ущерба, требовать его возмещения от Исполнителя, в т. ч. в судебном порядке
- Исполнитель обязуется ознакомить своих работников и сотрудников, привлекаемых третьих лиц с требованиями Положения.

2. Требования к Исполнителю

2.1. Исполнитель обязан:

- Предоставить запрашиваемые документы, касающиеся информационной безопасности Исполнителя, заполнить анкету и направить в адрес Заказчика в течение 10 (десяти) рабочих дней с момента получения запроса от Заказчика.
- В срок не более 5 рабочих дней, после получения замечаний, касающихся информационной безопасности Исполнителя, предоставить план исправления замечаний, с указанием назначенных ответственных и сроков устранения по каждому замечанию.
- В срок не более 20 рабочих дней предоставить отчет об исправлении замечаний касающихся информационной безопасности Исполнителя.

2.2. Доступ на объекты

- Доступ разрешён только сотрудникам Исполнителя, прошедшим согласование с Заказчиком.
- Сотрудники Исполнителя обязаны иметь при себе удостоверение личности и пропуск (если требуется).

2.3. Обращение с информацией

- Не фотографировать, не копировать и не передавать третьим лицам информацию, документы или оборудование Заказчика.
- Не обсуждать детали работы и внутренние процессы Заказчика с посторонними.

2.4. Использование техники и сетей

- Не использовать оборудование и сети Заказчика без разрешения.
- Не подключать свои устройства к сетям и оборудованию Заказчика.

2.5. Физическая безопасность

- Не оставлять без присмотра помещения, в которых ведутся работы.
- Сообщать Заказчику обо всех замеченных нарушениях или подозрительных ситуациях.

3. Субподрядчики/ субпоставщики

В случае, если условия Договора включают право привлечения Исполнителем третьих лиц, то соблюдаются следующие условия:

- Привлекаемые третьи лица обязаны соблюдать все требования Положения;
- Исполнитель обязан предоставить письменное подтверждение ознакомления любых третьих лиц, привлекаемых Исполнителем для оказания услуг по Договору.
- Исполнитель не реже, чем ежегодно должен оценивать соблюдение требований данного Положения, Договорных обязательств и SLA со стороны третьих лиц и предоставлять информацию Заказчику по запросу.
- Запрещено самостоятельное подключение Исполнителем третьих лиц к ИТ-инфраструктуре Заказчика и/или предоставление доступа к Информационным системам Заказчика без письменного согласования с Заказчиком;
- Доступ работников субподрядчика/субпоставщика к Информационным системам Заказчика, содержащим сведения, относимые к конфиденциальной информации, в рамках Договора не предоставляется. В случае необходимости передачи привлеченному третьему лицу защищаемой информации порядок такой передачи, условия передачи и обработки, требования к защите информации определяются отдельным договором между Заказчиком и привлеченным третьим лицом;
- Исполнитель несет полную ответственность за все действия и/или бездействия привлекаемых ими третьих лиц.

4. Протокол при выявлении нарушения безопасности (инцидента)

Исполнитель обязуется приложить все усилия, чтобы поспособствовать выявлению и предотвращению любых нарушений безопасности. Исполнитель должен соблюдать политику и процедуры реагирования на нарушения безопасности в соответствии с принятыми отраслевыми стандартами.

Исполнитель обязан информировать Заказчика обо всех фактах нарушения требований Положения или событиях, способных привести к таким нарушениям.

Стороны обмениваются информацией об инцидентах в свободном формате. Для повышения оперативности при передаче технической информации Стороны вправе использовать телефонную связь и иные каналы передачи информации. В рамках обмена информацией об инцидентах информационной безопасности Стороны не обмениваются информацией, содержащей персональные данные и иную информацию ограниченного доступа.

В случае нарушения безопасности или если Исполнитель обоснованно подозревает, что существует возможность нарушения безопасности или уже произошло, Исполнитель обязан:

- немедленно провести обоснованное расследование причин и обстоятельств, связанных с таким Нарушением безопасности;
- прилагать все усилия и предпринимать все необходимые действия для предотвращения и минимизации последствий такого нарушения безопасности;
- направить уведомление Заказчику в максимально короткий срок, но не позднее 24 часов с момента обнаружения данного факта через Ответственного со стороны Заказчика и/или по адресу cs@slb.ru;
- незамедлительно и ни в коем случае не позднее, чем через два (2) рабочих дня после даты, когда Исполнитель обнаружил или обоснованно заподозрил нарушение безопасности, предоставить Заказчику письменный отчет о таком Нарушении безопасности, включая список всех лиц, у которых есть или был доступ к Данным Заказчика;
- прилагать все усилия и предпринимать все необходимые действия для предотвращения и минимизации последствий такого нарушения безопасности;

В перечень инцидентов информационной безопасности Стороны включают инциденты, несущие риски потери конфиденциальности, целостности, доступности информации, в том числе:

• фишинговая атака якобы от имени Стороны;
• эксплуатация выявленной уязвимости на ресурсе, принадлежащем Стороне;
• эксплуатация выявленной уязвимости в программном обеспечении, предоставляемом/эксплуатируемом Стороной;
• заражение ВПО;
• НСД к ресурсам Стороны;
• DDOS-атака на ресурсы Стороны – выявленная, закончившаяся или планируемая.

При возникновении в инфраструктуре Исполнителя значимого инцидента информационной безопасности, последствия которого могут затронуть интересы Заказчика (в том числе клиентов или партнеров Заказчика), Исполнитель обязан известить об этом Заказчика в максимально возможный короткий срок, но не позднее 8 (восьми) часов с момента обнаружения такого инцидента (подозрения на инцидент).

Значимым считается инцидент информационной безопасности, удовлетворяющий одному из следующих критериев:

• невозможность выполнения Заказчиком бизнес-операций, в соответствии с установленными сроками, или ограничение функциональности ИТ-услуги или информационной системы Заказчика;

• разглашение аутентификационных данных или конфиденциальной информации (в том числе персональные данные);

• воздействие вредоносного программного обеспечения (далее – «ВПО»), массовые блокировки учетных записей, создание несанкционированных учетных записей;

• выявленные признаки несанкционированного доступа (далее – «НСД») или неудачных попыток получения НСД, а также злоупотребление привилегиями.

В случае устранения значимого инцидента информационной безопасности Исполнитель обязан уведомить Заказчика о мерах, предпринятых для управления инцидентом в течение 24 часов.

Кроме того, если Заказчик уведомлен о каком-либо нарушении безопасности или иным образом обнаруживает или подозревает, что Исполнитель пострадал от нарушения безопасности, по запросу Заказчика Исполнитель должен предоставить любые запрошенные документы, связанные с таким нарушением безопасности, включая, помимо прочего, любые отчеты об аудите оценки безопасности и контроля безопасности, журналы и любой судебный анализ такого нарушения безопасности. Исполнитель будет сотрудничать с Заказчиком в поисках судебного запрета или другого вида обеспечения защиты против любого такого лица, которое считается

ответственным или соучастником нарушения безопасности или кибератаки. В случае нарушения безопасности или кибератаки Исполнитель должен предпринять все необходимые корректирующие действия при взаимодействии с Заказчиком.

В случае появления новых типов инцидентов информационной безопасности, способов и механизмов их выявления, а также при необходимости оптимизации взаимодействия или изменения форматов передаваемых файлов, в Договор Сторон вносятся необходимые изменения (дополнения).

5. Конфиденциальность

Исполнитель признает, что при выполнении Заказа/Договора любая информация о Заказчике или его аффилированной компании, раскрытая Исполнителю или полученная Исполнителем в результате указанного выполнения, будет считаться конфиденциальной и принадлежащей Заказчику («Конфиденциальная Информация»). Не смотря на вышеизложенное, данный Договор, все Заказы и условия настоящего Договора считаются конфиденциальными и принадлежащими Заказчику, и могут быть использованы Заказчиком, как он сочтет нужным.

Исполнитель обязуется:

- рассматривать в качестве конфиденциальной, и
- в любое время в течение срока действия Договора и в течение последующих пяти (5) лет, не раскрывать, не распространять, не публиковать, не копировать, не воспроизводить, не продавать, не передавать в пользование, не обрабатывать, или иным образом не использовать (кроме как для целей выполнения Заказа/Договора, при условии, что информация раскрывается сотрудникам Компании по принципу служебной необходимости), или не разрешать использование любой Конфиденциальной Информации, кроме как с письменного согласия Заказчика.

Все вышеизложенное не применяются к любой Конфиденциальной Информации, которая:

(a) ранее была известна Компании на момент раскрытия информации от Заказчика или его Аффилированной компании, что может быть документально подтверждено,

(b) была самостоятельно разработана Исполнителем без нарушения Договора, или

(c) законно получена от третьей стороны без ограничения на использование или раскрытие информации, или

(d) которая во время ее раскрытия была общедоступна или которая после ее раскрытия становится общедоступной на законных основаниях, но не в результате действий или упущений Компании. В случае, если Исполнитель обязан раскрыть Конфиденциальную Информацию в соответствии с решением или иным постановлением суда, или иного компетентного органа государственной власти / местного самоуправления, обязательства Компании будут определяться в соответствии с пунктом далее.

- Исполнитель должен проявлять ту же степень осторожности, чтобы избежать несанкционированного разглашения Конфиденциальной Информации, какую она проявляет в отношении собственной конфиденциальной/служебной информации схожего качества и происхождения, но используя, по меньшей мере, разумные регламенты безопасности. В случае несанкционированного раскрытия Конфиденциальной Информации, Исполнитель немедленно уведомит Заказчика по обнаружении любого несанкционированного использования или разглашения Конфиденциальной Информации, и окажет сотрудничество любым разумным способом, чтобы помочь вернуть владение Конфиденциальной Информацией и предотвратить дальнейшее несанкционированное использование или разглашение.
- Под разглашением конфиденциальной информации в рамках текущего Положения понимается действие или бездействие одной из Сторон, в результате которого конфиденциальная информация становится известной третьим лицам в отсутствие согласия на это владельца конфиденциальной информации. При этом форма разглашения конфиденциальной информации третьим лицам (устная, письменная, с использованием технических средств и др.) не имеет значения.
- Исполнитель прямо признает, что предоставление информации со стороны Заказчика не предоставляет Исполнителю любых иных прав, кроме как ограниченного права использовать Конфиденциальную Информацию для выполнения Заказа/Договора (и ничего, содержащейся в настоящем документе не может быть истолковано как предоставление или присуждение каких-либо прав на торговые марки, изобретения, авторские права, патенты Заказчика и т.п.).
- По истечении или прекращении действия Договора по любой причине, Исполнитель обязан вернуть всю Конфиденциальную Информацию Заказчику (за исключением данного Договора и Заказов к нему), и не вправе делать или сохранить ее копии.
- Исполнитель гарантирует не хранить конфиденциальную информацию Заказчика в общедоступных ресурсах, не передавать ее за пределы Информационной инфраструктуры Заказчика в открытом (незащищенном от доступа посторонних лиц) виде, не использовать для передачи частной и конфиденциальной информации общедоступные интернет-мессенджеры (Viber, WhatsApp, Telegram, Skype и т.д.).

- Исполнитель не должен рекламировать или публиковать факт того, что Заказчик заключил Договор или Заказ с Заказчиком, а также использовать имя Заказчика в любой рекламе, публикациях, брошюрах или на сайте.

- В том случае, если Исполнителю или её Персоналу предлагается или требуется (посредством устных вопросов, опросных листов, запроса о предоставлении информации или документов, в ходе судебного разбирательства, повестки в суд, требования о возможности ознакомления с документами или иных подобных процессов) разгласить Конфиденциальную Информацию Заказчика, Исполнитель должен направить Заказчику оперативное письменное уведомление, если это допускается, о любой такой просьбе или требовании, так чтобы Заказчик мог обратиться за законными средствами для охраны конфиденциальности. Если в отсутствие законных средств для охраны конфиденциальности, Исполнитель или кто-либо из её Персонала, тем не менее, юридически вынуждены раскрыть Конфиденциальную Информацию Заказчика какому-либо суду или иному компетентному органу государственной власти / местного самоуправления, Исполнитель или её Персонал могут раскрыть такому суду/органу только ту часть Конфиденциальной Информации Заказчика, которая считается необходимой для раскрытия по закону.

- Раскрытие Конфиденциальной Информации Заказчика, не освобождает Исполнителя обязательств по защите раскрытой Конфиденциальной Информации от дальнейшего раскрытия Компанией или её Персоналом.

6. Ответственность Исполнителя за неисполнение/ненадлежащее исполнение условий Положения

Таблица № 1 «Нарушение исполнения условий Положения»:

№ п/п	Описание нарушения	Ответственность	Примечание
1	Выявленное нарушение пункта Положения	неустойка* 100000 рублей	за каждый факт

*Неустойка взыскивается сверх суммы документально подтвержденных убытков.