Общество с ограниченной ответственностью «Интегрити Солюшнс»

ОБЯЗАТЕЛЬСТВО

О СОБЛЮДЕНИИ ТРЕБОВАНИЙ КИБЕРБЕЗОПАСНОСТИ

Я, Домрачев Анатолий Иванович, являясь работником ООО «Интегрити Солюшнс», адрес (юридический): Российская Федерация, 127434, Москва, Дмитровское шоссе, д. 9, стр. 3, этаж 2, помещение I, комната 47 (далее – «Контрагент»), обязуюсь выполнять перечисленные ниже требования:

1. Использовать предоставленный мне доступ к автоматизированным системам (АС) Заказчика, оборудованию, средствам вычислительной техники (СВТ) и помещениям исключительно в целях исполнения обязательств по заключенным Контрагентом с Заказчиком договорам (далее – «Работы»/«Услуги»).

2. Не разглашать и не использовать в личных целях и целях третьих лиц конфиденциальную информацию Заказчика, доступ к которой предоставлен мне для проведения Работ, соблюдать требования режима коммерческой тайны Заказчика.

3. Не обсуждать на форумах и в конференциях сети Интернет вопросы, касающиеся моей профессиональной деятельности в части отношений с Заказчиком и его работниками.

4. Препятствовать ознакомлению посторонних лиц с конфиденциальными документами Заказчика, не допускать утрату (кражу, порчу, утерю) материальных носителей (USB-носителей, оптических дисков, внешних жестких дисков и др.), содержащих конфиденциальную информацию Заказчика.

5. Не хранить конфиденциальную информацию Заказчика в общедоступных ресурсах, не передавать ее за пределы сетей Заказчика в открытом (незащищенном от доступа посторонних лиц) виде, не использовать для передачи конфиденциальной информации общедоступные интернет-мессенджеры (Viber, WhatsApp, Telegram, Skype и т.д.).

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

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

8. При работе с СВТ Заказчика:

8.1. Оставляя рабочее место, блокировать его (комбинацией Win+L для систем под управлением Windows или Command+Control+Q для систем с Mac OS).

8.2. Не прерывать сканирование антивирусным программным обеспечением съемных машинных и медиа носителей информации (USB-носителей, оптических дисков, внешних жестких дисков и др.) при их подключении к автоматизированному рабочему месту (АРМ), включенному в сеть Заказчика.

8.3. Соблюдать парольную политику в части удовлетворения следующим требованиям:

- длина пароля должна быть не менее 8 символов;
- пароль должен содержать в себе символы как минимум трех категорий из четырех: буквы нижнего регистра (от a до z), буквы верхнего регистра (от A до Z), цифры (от 0 до 9) и спецсимволы (например: $, #, %);
- пароль не должен совпадать с логином и повторять предыдущие 4 пароля для данной учетной записи пользователя;
- пароль не должен включать осмысленные слова, словосочетания, общепринятые аббревиатуры, а также основываться на доступных данных о пользователе (фамилии, дате рождения, именах родственников, номеров телефонов и др.) или легко угадываемом алгоритме смены (Smi1le!, Smi2le!, Smi3le! и т.д.);
- пароль не должен содержать широко известные или легко угадываемые слова и последовательности символов (12345678, password, qwerty, aaabbb и т.д.)
- пароль по умолчанию (созданный при создании учетной записи пользователя) должен быть изменен пользователем при первом входе;
- пароль должен изменяться не реже чем 1 раз в 40 дней с момента последнего изменения;
- в случае разглашения или компрометации пароль должен быть незамедлительно изменен.

8.4. Соблюдать следующие 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 учетных записей;
- не передавать кому-либо (в т.ч. своим коллегам и руководителям, а также работникам Заказчика) свой пароль, равно как и использовать чужие пароли для работы с СВТ и АС Заказчика;
- не осуществлять попытки подбора паролей (в том числе автоматизированными способами), не пытаться завладеть паролями других лиц.

8.5. Не организовывать на предоставленном компьютере ресурсы общего доступа и сетевые сервисы (открывать доступ к общим папкам, дискам, CD-приводам и дисководам, настраивать

службы удаленного доступа, прокси- или веб-серверы, беспроводные точки доступа, Bluetooth интерфейсы и т.д.).

8.6. Не предпринимать попытки преодоления установленных Заказчиком ограничений, отключать и/или удалять установленные на предоставленных СВТ Заказчика средства защиты информации (в том числе антивирусное программное обеспечение), использовать недокументированные свойства, ошибки в программном обеспечении и настройках защиты доступа к информационным ресурсам и АС Заказчика, доступ к которым не был предоставлен явным образом.

8.7. Не устанавливать на предоставленные СВТ Заказчика какое-либо программное обеспечение кроме программного обеспечения, принятого в ФПД Заказчика, изменять настройки уже имеющегося. По вопросам установки необходимого программного обеспечения, а также получения административных прав в операционных системах персональных компьютеров обращаться к ответственному лицу Контрагента (для дочерних и зависимых обществ Заказчика) или Заказчика, назначенному в соответствии с Положением о соблюдении требований кибербезопасности.

8.8. Не хранить и не использовать на предоставленном компьютере программное обеспечение, фонограммы и другие результаты интеллектуальной деятельности в нарушение прав их законных правообладателей.

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

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

8.10. Не переходить по коротким ссылкам вида bit.ly или goo.gl.

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

8.12. Не подключать к предоставленным СВТ Заказчика личные мобильные устройства (телефоны, смартфоны, планшетные компьютеры, ноутбуки), беспроводные (радио) интерфейсы, модемы и прочее оборудование, позволяющее выходить в сеть Интернет и другие публичные сети.

9. Не использовать программное обеспечение следующих категорий при подключении к корпоративной сети Заказчика :

- сканеры портов и анализаторы трафика;

- средства для организации удаленного доступа, не утвержденные требованиями Заказчика, включая средства для создания зашифрованных каналов связи (VPN-, DNS-, SSH-, HTTPS-туннели и пр.) ;

- Программное обеспечение, используемое для анонимного доступа в сеть Интернет (включая веб-сервисы, прокси-серверы);

- Программное обеспечение для обхода средств защиты, включая средства подбора и восстановления паролей, поиска уязвимостей;

- Программное обеспечение, предназначенное для сокрытия или внедрения дополнительной информации в цифровые объекты (в том числе реализующее методы стеганографии);

- Программное обеспечение, осуществляющее сбор информации с клавиатуры, экрана, микрофона (снифферы);

- специализированные программные средства, оказывающее влияние на сетевые настройки СВТ, серверов и сетевого оборудования.

10. Не рассылать с корпоративных почтовых адресов Заказчика сообщений развлекательного, рекламного и иного характера, не относящегося к исполнению обязательств по заключенным с Заказчиком договорам.

11. Не использовать АРМ Заказчика (в том числе с использованием расширений к web-браузеру) и личные СВТ, подключенные к сетям Заказчика, 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.

12. Не оставлять без присмотра или передавать кому-либо предоставленные ТМ-идентификаторы, пропуска и прочие средства идентификации, а также ключи от помещений Заказчика.

13. По требованию уполномоченных представителей Заказчика предоставлять выданные СВТ Заказчика и носители информации (USB-Flash, CD/DVD и др.) для проверки выполнения требований информационной безопасности.

14. Информировать ответственное лицо Заказчика по вопросам кибербезопасности обо всех Инцидентах КБ и событий, создающих угрозу причинения ущерба Заказчику, а также об обращениях третьих лиц с целью незаконного получения конфиденциальной информации Заказчика.

Я предупрежден(а) о том, что, Заказчик вправе контролировать мои действия при работе с АС Заказчика, оборудованием и СВТ, включая анализ отправленных мной информационных сообщений, в т.ч. с использованием корпоративных почтовых систем Заказчика и с использованием сети Интернет.

Я предупрежден(а) о том, что Заказчик вправе использовать полученную в результате такого анализа информацию для проведения расследований, в том числе, с привлечением правоохранительных органов, а также использовать в качестве доказательств в суде, и подтверждаю, что в этих случаях я не вправе рассчитывать на соблюдение в отношении этих сообщений конфиденциальности со стороны Заказчика.

Я понимаю, что в случае выявления нарушений требований, перечисленных в настоящем Обязательстве, повлекших причинение ущерба Заказчику, Заказчик вправе отстранить меня от Работ/Услуг, приостановить мой доступ к своим АС, оборудованию, СВТ и в помещения Заказчика, а в случае подтверждения факта ущерба, требовать его возмещения Контрагентом, в т.ч. в судебном порядке.

С выпиской из УК РФ (ст.146, 183, 272, 273 и 274) ознакомлен(а). С перечнем информации, составляющей коммерческую тайну, и режимом коммерческой тайны Заказчика ознакомлен(а) и обязуюсь исполнять.

Настоящее Обязательство составлено в 2 (двух) экземплярах, по 1 (одному) для Заказчика и

_____.

«____» _____ 20___ _____/_____

(подпись)/(ФИО)