ТРЕБОВАНИЯ О КИБЕРБЕЗОПАСНОСТИ ПРИ ПРЕДОСТАВЛЕНИИ ТРУДА РАБОТНИКОВ (ПЕРСОНАЛА)

Настоящий документ устанавливает обязательные требования и рекомендации, предъявляемые YADRO к Компаниям (при предоставлении труда работников (персонала)) необходимые для обеспечения информационной безопасности и защиты интересов YADRO при использовании Компаниями информационных активов YADRO и исполнении заключенных Договоров.

Термины, определения и сокращения

ИБ (Информационная Безопасность) — состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

IT-ресурсы — оборудование, программное обеспечение, сети и другие системы, предназначенные для хранения, обработки и передачи информации YADRO.

АРМ — автоматизированное рабочее место.

Дистрибутив — форма распространения программного обеспечения.

Договор — любой Договор, Сделка, Контракт или иное Соглашение между YADRO и Компанией.

Документы по ИБ YADRO — документы YADRO, регулирующие требования к обеспечению информационной безопасности.

Исполняющие работники или Пользователи — сотрудники Компании, привлеченные Компанией к оказанию услуг /выполнению работ по Договору.

Инцидент ИБ — непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (может привести) к нарушению функционирования IT-ресурса или возникновению угроз безопасности информации или нарушению требований по защите информации одно или несколько нежелательных или неожиданных событий информационной безопасности, которые со значительной степенью вероятности приводят к компрометации операций бизнеса и создают угрозы для информационной безопасности.

YADRO — сторона 1 (YADRO).

Компания — сторона 2 (Контрагент YADRO по Договору).

1. Предмет Требований

1.1. Настоящие требования по информационной безопасности при предоставлении труда работников (персонала) (далее — «Требования о ИБ») определяют обязательные для Компаний меры и рекомендации по информационной безопасности, предъявляемые при выполнении Компанией работ в сфере информационных технологий и/или информационной безопасности, а также при предоставлении Компании доступа к IT-ресурсам YADRO. Положения настоящих требований по информационной безопасности применяются в той части, в которой они напрямую применимы и относятся к конкретным видам работ или услуг, выполняемых (оказываемых) Компанией по договорам с YADRO. Указанные Требования о ИБ не являются исчерпывающими и могут быть дополнены или уточнены с учётом характера оказываемых услуг, выполняемых работ и специфики деятельности Компании.

2. Ознакомление с документами по информационной безопасности

2.1. До получения доступа в офисное помещение и к IT-ресурсам YADRO Компания обязана ознакомить всех исполняющих работников, привлекаемых к выполнению работ по Договору, с документами YADRO, регулирующими требования к обеспечению информационной безопасности (далее — «Документы по ИБ»).

2.2. Компания гарантирует, что все исполняющие работники, привлекаемые к исполнению Договоров, надлежащим образом ознакомлены с Документами по ИБ в соответствии с п. 2.1 Требований о ИБ. Компания обязуется проводить инструктажи по обеспечению безопасности исполняющих работников, задействованных в оказании услуг /выполнении работ по Договору. По запросу YADRO Компания обязана предоставить документы, подтверждающие факт ознакомления исполняющего работника с Документами по ИБ, в сроки, указанные в запросе YADRO.

2.3. Компания обязана не допускать к оказанию услуг /выполнению работ по Договору работников, которые не ознакомлены с Документами по ИБ и/или отказались от ознакомления с Документами по ИБ.

3. Исполнение требований информационной безопасности

3.1. Исполняющие работники обязаны строго соблюдать все требования Документов по ИБ, а также меры информационной безопасности, предусмотренные Документами по ИБ.

3.2. В случае оказания услуг /выполнения работ по Договору на территории YADRO, во время отсутствия в офисном помещении, или при покидании места оказания услуг /выполнения работ, Исполняющие работники обязаны заблокировать сеанс учетной записи пользователя на АРМ для исключения несанкционированного доступа.

3.3. В случае предоставления YADRO средств вычислительной техники в рамках выполнения работ, оказания услуг в сфере информационных технологий и/или информационной безопасности, а также при предоставлении Компании удаленного доступа к информационным ресурсам YADRO, Компании (в т.ч. Исполняющим работникам) запрещается:

3.3.1. предпринимать попытки преодоления установленных YADRO ограничений, отключать и/или удалять установленные на предоставленных средствах вычислительной техники YADRO средств защиты информации (в том числе антивирусное ПО), использовать недокументированные свойства, ошибки в ПО и настройках защиты доступа к информационным ресурсам YADRO, доступ к которым не был предоставлен явным образом;

3.3.2. устанавливать на предоставленные средства вычислительной техники YADRO какое-либо ПО, изменять настройки уже имеющегося. По вопросам установки необходимого ПО, а также получения административных прав в операционных системах персональных компьютеров обращаться в отдел информационных технологий YADRO;

3.3.3. организовывать на предоставленном средстве вычислительной техники 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.);

3.3.4. хранить и не использовать на предоставленном компьютере ПО и другие результаты интеллектуальной деятельности в нарушение прав их законных правообладателей;

3.3.5. подключать к предоставленным средствам вычислительной техники YADRO мобильные устройства (телефоны, смартфоны, планшетные компьютеры, ноутбуки), беспроводные (радио) интерфейсы, модемы и прочее оборудование, позволяющее выходить в сеть Интернет и другие публичные сети.

3.4. Исполняющим работникам категорически запрещено отключать, изменять или ограничивать функционал любых средств защиты информации, развернутых на IT-ресурсах YADRO, включая, но не ограничиваясь следующими мерами:

3.4.1. отключение или модификация антивирусного программного обеспечения;

3.4.2. отключение или модификация систем обнаружения и предотвращения вторжений (IDS/IPS);

3.4.3. отключение или модификация брандмауэров и других систем контроля сетевого трафика;

3.4.4. отключение или изменение параметров журналирования (логирования) систем безопасности;

3.4.5. отключение или изменение настроек систем шифрования данных;

3.4.6. отключение контроля целостности программного обеспечения и данных.

3.5. Исполняющим работникам категорически запрещено:

3.5.1. пытаться самостоятельно расширить предоставленные права;

3.5.2. использовать информационные ресурсы YADRO, к которым предоставлен доступ, для совершения незаконных действий;

3.5.3. предоставлять доступ к полученной информации третьим лицам;

3.5.4. осуществлять раскрытие, разглашение, копирование и распространение результатов использования информационных ресурсов YADRO без специального письменного согласия YADRO.

3.6. Нарушение любого из требований разделов 2-3 Требований о ИБ считается существенным нарушением обязательств Компании и может повлечь за собой применение штрафных санкций в соответствии с разделом 6 ниже.

4. Аудиты информационной безопасности

4.1. YADRO вправе проводить аудиты информационной безопасности, в том числе в отношении Исполняющих работников, для проверки соблюдения ими требований по информационной безопасности. YADRO уведомляет Компанию о планируемом аудите не менее чем за 5 (пять) рабочих дней до даты начала аудита информационной безопасности.

4.2. В ходе аудитов исполняющие работники обязаны предоставлять YADRO всю необходимую информацию по его запросу и содействовать проведению аудитов.

4.3. В случае выявления нарушений требований информационной безопасности исполняющими работниками, Компания обязана незамедлительно устранить выявленные недостатки и предпринять все необходимые действия в соответствии с требованиями/запросом YADRO.

5. Требования к АРМ для работы с информационными системами YADRO

5.1. На АРМ, предоставленных Компании для осуществления доступа к сети и IT-ресурсам YADRO, по умолчанию установлено следующее обязательное ПО (далее — «Обязательное ПО»):

5.1.1. агент Kaspersky Security Center (WIN / MAC / Linux);

5.1.2. Wazuh agent (WIN / MAC / Linux);

5.1.3. Anscible (применимо только для Linux);

5.1.4. IRP (применимо только для Linux);

5.1.5. ManageEngine UEMS — Agent (WIN / MAC / Linux).

5.2. Дистрибутивы Обязательного ПО выдаются YADRO в составе средств вычислительно техники в момент предоставления средств вычислительной техники Компании.

5.3. В случае удаления Компанией Обязательного ПО с предоставленных YADRO средств вычислительной техники, YADRO вправе ограничить доступ к сети и информационным системам.

6. Ответственность за нарушение требований информационной безопасности

6.1. Компания несет ответственность за нарушения установленных настоящими Требованиями о ИБ мер по информационной безопасности Исполняющими работниками.

6.2. За каждый выявленный случай нарушения требований информационной безопасности со стороны Исполняющих работников, YADRO вправе потребовать от Компании оплаты неустойки (штрафа).

6.3. В случае систематических (т.е. два и более нарушений в течение срока действия Договора) нарушений требований информационной безопасности со стороны Исполняющих работников YADRO имеет право отказаться от исполнения Договора в одностороннем порядке с уведомлением Компании в письменной форме, а также право требовать от Компании возмещения убытков в полном объеме.