|  |
| --- |
| *Приложение № 1* |
| *к договору об оказании услуг*  *№ИСО\_2016 от \_\_\_ \_\_\_\_\_\_\_\_2016г.* |

**Порядок взаимодействия**

**Заказчика и Исполнителя по обеспечению безопасности**

**информационных ресурсов Заказчика.**

1. **Общие положения.**
   1. Общее руководство и принятие всех решений по вопросам обеспечения режима коммерческой тайны, конфиденциальности и информационной безопасности Исполнителя осуществляет руководитель Исполнителя.
   2. Организацию мероприятий по обеспечению режима коммерческой тайны, конфиденциальности и информационной безопасности Исполнителя осуществляет подразделение безопасности Исполнителя.
   3. Исполнитель должен разработать и соблюдать требования локальных нормативных документов по вопросам коммерческой тайны, конфиденциальности и информационной безопасности.
   4. Для выполнения технологических операций по обеспечению режима коммерческой тайны, конфиденциальности и информационной безопасности Исполнителя, из числа штатных работников Исполнителя назначаются ответственные за информационную безопасность, также допускается выполнение технологических операций по обеспечению безопасности на договорной основе сторонними организациями, согласованными с Заказчиком.
   5. Заказчик оставляет за собой право по контролю обеспечения режима коммерческой тайны, конфиденциальности и информационной безопасности, а также участвовать в проведении совместных проверок и расследований по признакам и фактам нарушения Исполнителем требований безопасности, закрепленных договором и приложениями к нему.
2. **Безопасность рабочих мест.**
   1. Для обеспечения своей деятельности Исполнитель обязан использовать только лицензионное и официально приобретенное оборудование и программное обеспечение. Применение бесплатного или условно бесплатного программного обеспечения должно согласовываться со Службой безопасности Заказчика.
   2. Для доступа к информационным ресурсам Заказчика Исполнитель может использовать программное обеспечение, предоставленное только Заказчиком. Использование иного программного обеспечения должно согласовываться с Заказчиком. Исполнитель не вправе вносить любые изменения в предоставляемое Заказчиком программное обеспечение.
   3. Настройки политик безопасности операционной системы рабочих мест, с которых осуществляется доступ к информационным ресурсам Заказчика, должны соответствовать политикам, принятым в КИВС Заказчика.
   4. На рабочих местах Исполнителя, с которых осуществляется доступ к информационным ресурсам Заказчика, использование программного обеспечения, не предназначенного для организации данного доступа, требует обязательного согласования с Заказчиком.
   5. Права пользователя на рабочем месте должны быть ограничены и не должны позволять осуществлять действия по изменению программно-аппаратного обеспечения.
   6. Права на изменения программно-аппаратного обеспечения, а также заведение новых пользователей и назначение им полномочий в системе, должны иметь специально назначенные работники ИТ-подразделения Исполнителя.
   7. Применяемое Исполнителем системное программное обеспечение должно своевременно обновляться с использованием автоматизированных средств обновлений.
   8. Запрещается хранение конфиденциальной информации Заказчика на неучтенных носителях информации, а также на жестких дисках рабочих станций Исполнителя, с которых осуществляется доступ к информационным ресурсам сторонних организаций и в сеть общего пользования Интернет.
   9. Сегменты сетей Исполнителя и Заказчика должны быть разделены средствами межсетевого экранирования с проведением строгой политики управления доступом, в соответствии с политикой, принятой к КИВС Заказчика, в целях исключения доступа к неразрешенным объектам, а также использования неразрешенных протоколов, сервисов и служб.
3. **Доступ к информационным ресурсам.**
   1. Аутентификация пользователя Исполнителя при доступе к информационным ресурсам Заказчика должна осуществляться с использованием механизмов усиленной двухфакторной аутентификации (с применением цифровых сертификатов). В отдельных случаях (система не поддерживает двухфакторную аутентификацию) возможно применение уникального персонального идентификатора и пароля. Парольная политика должна соответствовать требованиям, принятым в КИВС Заказчика.
   2. Доступ к информационным ресурсам Заказчика должен осуществляться только по доверенным каналам связи, принадлежащим Заказчику, в противном случае должны применяться механизмы шифрования на сетевом уровне. При применении шифрования должны использоваться алгоритмы шифрования, принятые Заказчиком, ключи шифрования, выданные Службой безопасности Заказчика.
   3. Доступ к информационным ресурсам Заказчика предоставляется только штатным работникам Исполнителя на основании заявки оформленной Исполнителем, подписанной руководителем подразделения Исполнителя, согласованной Службой безопасности Исполнителя, руководителем подразделения Заказчика - владельцем ресурса, ИТ-подразделением Заказчика и Службой безопасности Заказчика.
   4. Заявка на доступ к информационным ресурсам должна содержать: наименование информационного ресурса, необходимые права на доступ, ФИО пользователя, подразделение, должность, местонахождение рабочего места, контактный телефон, сетевой идентификатор пользователя (ей), DNS-имя компьютера (список) с которого будет осуществляться доступ.
   5. Доступ работникам Исполнителя к информационным ресурсам Заказчика предоставляется исключительно для выполнения обязательств, предусмотренных договором.
   6. Доступ предоставляется минимально необходимый для выполнения работником своих должностных обязанностей. Ответственность за обоснованность запрашиваемого доступа возлагается на руководителя подразделения Исполнителя, запросившего доступ.
   7. Централизованный учет пользователей информационных ресурсов Заказчика и его своевременная актуализация возлагается на ИТ-подразделение Исполнителя. Учет сотрудников Исполнителя, допущенных к конфиденциальной информации, а также проведение служебных расследований по фактам нарушений требований информационной безопасности возлагается на Службу безопасности Исполнителя, с привлечением Службы безопасности Заказчика.
   8. Уволенные работники Исполнителя должны быть лишены допуска ко всем ресурсам (без исключения). Ответственность за своевременное лишение допуска возложена на руководителя, оформившего допуск. В целях своевременного лишения допуска к информационным ресурсам Заказчика, руководитель подразделения Исполнителя, оформивший допуск информирует ИТ-подразделение Заказчика не позднее 3 дней после подачи заявления об увольнении с указанием фактической даты прекращения допуска. Подразделение по работе с персоналом Исполнителя не реже 1 раза в месяц информирует Службу безопасности Заказчика об уволенных работниках и работниках, переведенных на другие должности.
   9. Исполнитель должен обеспечивать журналирование (логирование) доступа своих работников к информационным ресурсам Заказчика и по требованию предоставлять эту информацию Службе безопасности Заказчика.
   10. Заказчик оставляет за собой право контролировать действия работников Исполнителя при осуществлении доступа к информационным ресурсам Заказчика и приостанавливать доступ в случаях возникновения ситуаций, создающих угрозу информационной безопасности Заказчика, уведомив об этом Исполнителя. Доступ восстанавливается после устранения выявленной угрозы на основании заявки согласованной со Службой безопасности Заказчика.
4. **Реагирование на инциденты информационной безопасности.**
   1. Исполнитель должен информировать Службу безопасности Заказчика обо всех случаях возникновения инцидентов информационной безопасности.
   2. Исполнитель должен безотлагательно предпринимать все необходимые меры по предотвращению и минимизации ущерба при возникновении инцидента информационной безопасности.
   3. В случаях возникновения угроз информационной безопасности Заказчика со стороны сети, рабочих мест или пользователей Исполнителя, а также претензий со стороны государственных контролирующих органов или фактов нарушений, приведших к материальному ущербу, расследование осуществляет Служба безопасности Заказчика совместно со Службой безопасности Исполнителя.
5. **Применение средств защиты информации.**
   1. Установка средств защиты информации Исполнителем должна в обязательном порядке согласовываться со Службой безопасности Заказчика.
   2. Установка и ввод в эксплуатацию средств защиты информации должна осуществляться в соответствии с эксплуатационной и технической документацией.
   3. Исполнитель должен проводить обучение лиц, использующих средства защиты информации, правилам работы с ними.
   4. Учет применяемых средств защиты информации, эксплуатационной и технической документации и носителей конфиденциальной информации возлагается на ответственного работника Исполнителя.
   5. Контроль за соблюдением условий использования средств защиты информации возлагается на Службу безопасности Исполнителя.
   6. Средства защиты информации, применяемые Исполнителем, должны быть подключены к централизованной Системе мониторинга информационной безопасности Заказчика.
6. **Доступ в сеть Интернет.**
   1. Доступ в сеть общего пользования, Интернет с рабочих мест, с которых осуществляется доступ к информационным ресурсам Заказчика, должен осуществляться в соответствии с требованиями нормативных документов Заказчика по использованию сети Интернет.
   2. Доступ в сеть Интернет должен осуществляться только авторизованными пользователями через средства межсетевого экранирования, журналироваться автоматизированными средствами (Proxy-сервер), контролироваться антивирусным программным обеспечением и автоматизированными средствами обнаружения вторжений и аномалий (IDS). Политики безопасности указанных средств должны соответствовать требованиям Заказчика. Изменение политик безопасности должно согласовываться со Службой безопасности Заказчика.
   3. Контент-контроль доступа в сеть Интернет работниками Исполнителя осуществляет Служба безопасности Исполнителя.
   4. Взаимодействие работников Исполнителя с внешними контрагентами должно осуществляться только с использованием корпоративной электронной почты или специально организованных информационных систем.
   5. Передача конфиденциальной информации через сеть Интернет запрещена.
   6. Запрещается использование Интернета для своих личных целей, в том числе для посещения развлекательных, игровых, музыкальных, порнографических, террористических сайтов.
   7. Не допускается неуполномоченное представление личной точки зрения точкой зрения Заказчика или Исполнителя в сети Интернет.
   8. Не допускается оплата услуг пользователей онлайновых сервисов Интернет в личных целях с рабочих мест Исполнителя.
7. **Антивирусная безопасность.**
   1. В целях непрерывного и комплексного обеспечения Исполнителя системой антивирусной безопасности, все рабочие места и сервера Исполнителя должны быть оснащены лицензионным антивирусным программным обеспечением. За поддержание работоспособности антивирусного программного обеспечения и актуальности антивирусных баз назначается штатный работник Исполнителя или должен быть заключен договор на поддержку системы антивирусной безопасности.
   2. Система антивирусной безопасности Исполнителя должна стоять из трех уровней, каждый из которых должен иметь антивирусное программное обеспечение различных производителей:

- системы, которые непосредственно соединяются с сетью общего пользования;

- сервера: файловые, внутренние почтовые и серверах приложений;

- рабочие станции и сервера рабочих групп, удаленные или мобильные пользователи.

* 1. Система антивирусной безопасности должна иметь систему централизованного обновления и управления.
  2. В случае если рабочее место, с которого осуществляется доступ к информационным ресурсам Заказчика, невозможно оснастить антивирусным программным обеспечением, по согласованию со Службой безопасности Заказчика, на рабочем месте должна быть создана замкнутая программная среда, не позволяющая осуществлять запуск любых приложений, кроме штатных.

1. **Информационное взаимодействие.**
   1. В целях обеспечения авторства, целостности и юридической значимости, электронные документы, направляемые Исполнителем в адрес Заказчика, должны быть подписаны электронной цифровой подписью, в соответствии с порядком, принятым у Заказчика и требованиями законодательства Российской Федерации.
2. **Контроль состояния информационной безопасности.**
   1. В целях проверки выполнения требований по информационной безопасности, а также предупреждения и своевременного выявления нарушений информационной безопасности, в подразделениях Исполнителя должен осуществляться контроль состояния информационной безопасности Исполнителя.
   2. Контроль состояния информационной безопасности в подразделениях Исполнителя осуществляют Службы безопасности Исполнителя и Заказчика в соответствии с согласованными планами работ.
   3. Плановым проверкам должны подвергаться все подразделения Исполнителя не реже 1 раза в 3 года.
   4. Внезапные проверки проводятся Службой безопасности Исполнителя или Заказчика в соответствии с внутренними утвержденными планами работ.
   5. По фактам инцидентов информационной безопасности в обязательном порядке проводится внеплановая проверка состояния информационной безопасности Службой безопасности Исполнителя совместно со Службой безопасности Заказчика с целью выявления причин, устранения нарушений и предупреждения подобных нарушений в дальнейшем.
   6. Внеплановые проверки состояния информационной безопасности проводятся в обязательном порядке при реорганизации подразделений Исполнителя, изменения в технологии работы, состава программно-аппаратного обеспечения.
3. **Обучение персонала.**
   1. Исполнитель (иное лицо, привлеченное Исполнителем) должен всех вновь принимаемых работников знакомить под роспись с нормативными документами по вопросам информационной безопасности. Проводить регулярное обучение работников по вопросам информационной безопасности при предоставлении доступа к информационным ресурсам Заказчика. Доводить до работников новые нормативные документы под роспись.
   2. Не реже 1 раза в год проводить плановый Инструктаж по вопросам информационной безопасности.
   3. Заказчик обязуется проводить обучение работников Исполнителя ответственных за информационную безопасность не реже 1 раза в год.
4. **Ответственность.** 
   1. Работники Исполнителя (иных лиц, привлеченных Исполнителем), нарушившие действующие требования по информационной безопасности, и руководители подразделений, не обеспечившие их выполнение, привлекаются к дисциплинарной ответственности в соответствии с действующим трудовым законодательством.
   2. При подозрении на мошенничество или иные преступления, а также в случаях нанесения материального ущерба Заказчику, явившиеся следствием нарушения информационной безопасности, материалы предаются в правоохранительные органы.

|  |  |  |
| --- | --- | --- |
| **Заказчик**  ПАО «Башинформсвязь»  450000, г. Уфа, ул. Ленина, д.32/1  БИК 044030861  ИНН 0274018377  КПП 99775000  р/с 40702810900000005674  в ОАО АБ «Россия» г. Санкт-Петербург  к/с 30101810800000000861 в Северо-Западном Главном Управлении Банка России | **Исполнитель**   |  | | --- | | АО «МЦ НТТ»  119002, г. Москва Арбат,46, стр.1  БИК 044 583 119  ИНН 7704137364  КПП 770401001  р/с 4070 28зака10 9000 0009 9101 в ОАО «Промсвязьбанк»  к/с 3010 1810 6000 0000 0119 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_ Долгоаршинных М.Г.  МП | |  | | --- | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Петров А.Л.  МП | |