Приложение №1
к ТИПОВОМУ СОГЛАШЕНИЮ
о подключении и пользовании сервисами
государственной доверенной
инфокоммуникационной инфраструктуры
Республики Башкортостан

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Участника обмена

2016 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика информационной безопасности Участника обмена (далее – Политика ИБ) определяет требования к сотрудникам Участника обмена по обеспечению информационной безопасности при работе с информационными системами, информационными ресурсами и сервисами, предоставляемыми посредством государственной доверенной инфокоммуникационной инфраструктуры Республики Башкортостан (далее – сервисы ГДИИ РБ), а также описывают необходимые действия сотрудников по их соблюдению.

1.2. Положения настоящей Политики ИБ являются обязательными для соблюдения всеми сотрудниками Участника обмена, работающими с сервисами ГДИИ РБ.

1.3. Ознакомление сотрудников с настоящей Политикой ИБ осуществляется под роспись в установленном порядке.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Информационный ресурс (ИР)	– любое системное или прикладное программное обеспечение, физические и виртуальные хранилища данных в электронном виде, средства чтения и записи электронных носителей информации.
Мобильное устройство	– любое легко перемещаемое вычислительное устройство, предназначенное и используемое для создания, получения, хранения, обработки и передачи информации. К ним относятся ноутбуки (в том числе планшетные портативные компьютеры), карманные портативные компьютеры (КПК), смартфоны, компьютерные записные книжки, сотовые телефоны.
Корпоративное мобильное устройство	– мобильное устройство, являющееся собственностью Участника обмена.
Администратор информационной безопасности (АИБ)	– сотрудник Участника обмена, назначенный ответственными за обеспечение информационной безопасности, техническое взаимодействие и участие в определении и нейтрализации последствий инцидентов информационной безопасности, произошедших в зоне ответственности Участника обмена.

Носитель информации	– материальный предмет, на котором (или в котором) возможно разместить информацию в виде символов, образов, файлов и пр.
Съемный носитель информации	– электронный носитель информации, подключаемый к средствам компьютерной техники и используемый для хранения информации. К съемным носителям информации относятся дискеты, оптические (CD, DVD) диски, USB-носители, энергонезависимые карты памяти, фотоаппараты и т.п.
Съемный носитель ключевой информации (ключевой носитель)	– электронный носитель информации, на котором содержатся криптографические ключи для шифрования и электронной подписи документов. К съемным носителям ключевой информации относятся Touch Memory («таблетка»), RuToken/eToken (в виде USB-носителя), гибкий магнитный диск (дискета) и пр.
Устройство ввода-вывода информации	– выполненные как во внутреннем, так и во внешнем исполнении дисководы, приводы чтения и записи CD и DVD дисков, USB-порты и прочие переносные устройства, которые могут использоваться для выгрузки или загрузки информации в компьютер. Устройства ввода-вывода также являются информационными ресурсами.
Организация	– орган государственной власти Республики Башкортостан, орган местного самоуправления Республики Башкортостан, государственная организация, территориальное подразделение федерального органа исполнительной власти в Республике Башкортостан или иное юридическое лицо, подключенное к ГМС РБ.

3. НОРМАТИВНЫЕ ССЫЛКИ

3.1. В своей деятельности сотрудники Организации, в том числе АИБ, должны руководствоваться нормативными правовыми актами в области защиты информации, включая:

3.1.1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

3.1.2. Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

3.1.3. Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

3.1.4. Методический документ ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»;

3.1.5. Приказ ФСБ России от 10 июля 2014 г. №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

3.1.6. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

3.1.7. Приказ ФАПСИ от 13 июня 2001 г. №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

4. РАБОТА С ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО ДОСТУПА

4.1. Доступ к информации ограниченного доступа и ее передача

4.1.1. Сотрудники Участника обмена **обязаны не разглашать информацию ограниченного доступа** в течение всего времени работы в Организации, а также обязаны соблюдать требования законодательства Российской Федерации и Республики Башкортостан и внутренних нормативных документов Организации, регулирующих порядок предоставления информации, принадлежащей Организации, лицам, не являющимся сотрудниками Организации. Фактом разглашения информации ограниченного доступа является несанкционированное предоставление данной информации, лицам, не имеющим прав на доступ к данной информации. Сотрудники **несут ответственность** за несанкционированное разглашение им информации ограниченного доступа в соответствии с действующим законодательством Российской Федерации и Республики Башкортостан.

4.1.2. Разовое (единовременное) предоставление доступа к конфиденциальной информации либо ознакомление с ней сотрудников, характер должностных обязанностей которых не связан с ее получением, использованием или обработкой, допускается **только** по согласованию с руководителем подразделения, имеющего право предоставления доступа к данной информации.

4.1.3. Предоставление постоянного (на постоянной основе) доступа и доступ к сетевым информационным ресурсам осуществляется в соответствии с разделом 6 настоящей Политики ИБ.

4.1.4. Передача документов на любых носителях, содержащих информацию ограниченного доступа, третьим лицам (клиентам, контрагентам и др.) без согласования с вышестоящего руководителем подразделения и АИБ **запрещается**. При передаче необходимо удостовериться, что с получателем заключено Соглашение о неразглашении и защите конфиденциальной информации.

4.1.5. При работе с носителями информации, содержащими конфиденциальную информацию, сотрудник не должен оставлять данные носители без присмотра или должен убрать их в закрытое на ключ место хранения. Общие правила пользования, учета и хранения ключей от шкафов, тумбочек и прочих запирающихся устройств описаны в разделе 10 настоящей Политики ИБ.

4.1.6. Не допускается производить работу с **конфиденциальной** информацией в случае возможности ее просмотра посторонними лицами. Лица, не являющиеся сотрудниками, (например, посетители) не должны видеть конфиденциальную информацию на экране компьютера. При необходимости сотрудникам следует закрыть или свернуть все окна с конфиденциальной информацией или заблокировать компьютер. Бумажные конфиденциальные документы следует перевернуть текстом вниз или убрать со стола.

4.1.7. Делать копии, фотографировать или производить выписки из документов, содержащих конфиденциальную информацию, на любых видах носителей **не допускается**. Для осуществления данных действий необходимо получить **письменное** разрешение вышестоящего руководителя и разрешение АИБ.

5. РАБОТА С ПЕРСОНАЛЬНЫМ КОМПЬЮТЕРОМ

5.1. Сотруднику **запрещается** вскрывать персональный компьютер, который используется для работы (далее – компьютер), в том числе для самостоятельного устранения

неисправностей, или **подключать к компьютеру любое оборудование**, не связанное непосредственно с его должностными обязанностями (модем, личные карманные персональные компьютеры (КПК), смартфоны и сотовые телефоны и пр.).

5.2. При отсутствии сотрудника на рабочем месте даже на незначительный период времени (более 5 минут) сотрудник **обязан блокировать доступ к компьютеру**. Если сотрудник опасается забыть блокировать компьютер, то следует установить пароль на экранную заставку с интервалом не более 5 минут.

5.3. По окончанию рабочего дня сотрудник должен выключать персональный компьютер. Исключением являются случаи, когда существует обоснованная в силу выполнения должностных обязанностей служебная необходимость не выключать компьютер.

5.4. Сотруднику запрещается **самостоятельно устанавливать на компьютер программное обеспечение** (в том числе полученное в сообщениях электронной почты или из сети Интернет), изменять программную или аппаратную конфигурацию компьютера и настройки операционной системы. Список стандартного программного обеспечения и условия его установки для каждой категории сотрудника определяются иными нормативными и распорядительными документами Организации. В случае необходимости установки дополнительного ПО сотруднику необходимо оформить соответствующую заявку на ИР или служебную записку в соответствии с утвержденной процедурой управления правами доступа в Организации.

5.5. Сотруднику **запрещается отключать и/или удалять установленные средства защиты** (в том числе антивирусное программное обеспечение), а также изменять настройки данных средств.

5.6. Выполнение операций в ресурсах (прикладных системах), последствия которых сотруднику не известны в силу отсутствия знаний по работе с данным ресурсом, использование компьютера для мошенничества и других видов противозаконной деятельности, а также использование каких-либо средств для осуществления несанкционированного доступа к ресурсам Организации запрещается.

5.7. Самостоятельно осуществлять подключение, отключение, переключение и перенастройку сетевых элементов компьютера запрещается (подключение каких-либо сетевых карт, подключение компьютера в другую сетевую розетку и пр). Для проведения данных действий сотруднику необходимо обратиться в подразделение, ответственное за сопровождение рабочих мест Организации. Данный пункт не относится к сотрудникам, в обязанности которых входит перенастройка компьютеров.

6. ДОСТУП К ИНФОРМАЦИОННЫМ РЕСУРСАМ

6.1. Доступ к информационным ресурсам предоставляется сотрудникам **только** на основании соответствующих заявок, оформленных в соответствии с утвержденной процедурой управления правами доступа в Организации.

6.2. До начала работы в вычислительной сети Организации сотрудник обязан ознакомиться с настоящей Политикой ИБ.

6.3. Сотрудник **обязан** периодически производить смену используемых им паролей. Срок действия паролей для разных ИР может быть различным, однако смену пароля нужно осуществлять не реже чем 1 раз в 90 дней.

6.4. При создании пароля сотрудник должны выбирать **сложные пароли**, состоящие не менее чем из **8** символов и **обязательно** содержащие как буквы, так и цифры, и, по возможности, специальные знаки (!»№;%:?*()_ и т. п.). Пароль не должен быть очевидными, то есть содержаться в каком-либо словаре. Не следует использовать в качестве пароля свою фамилию, даты рождений, имена детей номера своих телефонов, паспортов и других документов и т.п., а также любые всем известные и/или легко угадываемые сокращения. Запрещается использовать в качестве пароля имя пользователя (идентификатор доступа).

6.5. Для создания надежных паролей рекомендуется использовать программные генераторы

паролей.

6.6. При создании пароля сотрудникам **запрещается** использовать пароли, применяемые ими для доступа к домашним компьютерам, бесплатным службам электронной почты, web-сайтам сети Интернет и прочим сервисам неслужебного характера.

6.7. **Запрещается** записывать пароли в доступных для визуального просмотра местах, а также хранить их в открытом виде на электронных носителях, за исключением ключевых носителей, к которым предъявляются отдельные требования (подробнее описано в разделе 8.3 настоящей Политики ИБ).

6.8. Сотрудникам **запрещается** передавать кому-либо (в том числе администраторам, непосредственному и вышестоящему руководителю) или разглашать свои аутентификационные данные (идентификатор доступа и пароль) для доступа к любому информационному ресурсу. Исключением могут быть случаи, когда отсутствие сотрудника на рабочем месте (например, при болезни, вынужденном отсутствии и т.п.) может привести к приостановлению работы подразделения. В этом случае, возможен сброс пароля. После выхода на работу сотрудник обязан сменить пароль, который был использован другим сотрудником, при первом доступе к ИР.

При проведении очередных проверок техники уполномоченными сотрудниками сотрудник должен **самостоятельно** вводить свой пароль. **В случае поступления запроса по телефону или электронной почте с просьбой сообщить аутентификационные данные, немедленно сообщить об этом непосредственному руководителю.**

6.9. Запрещается осуществлять доступ к ИР с использованием чужого идентификатора доступа (имя пользователя) и пароля (за исключением случаев, описанных в п. 6.8 настоящей Политики ИБ). Для доступа к ИР сотруднику следует использовать только персональный (собственный) идентификатор доступа и пароль. В случаях, когда технологически предусмотрено использование общих для нескольких сотрудников идентификаторов доступа, использование единого идентификатора возможно при обязательном согласовании с владельцем информационного ресурса. В этом случае руководитель подразделения является ответственным за контроль использования общего идентификатора доступа. Использовать несколькими сотрудниками одних и тех же персональных идентификаторов доступа в один промежуток времени запрещается.

6.10. Сотрудники, у которых доступ к информационным ресурсам организован с использованием электронных ключей, в том числе ключей электронной подписи, **не** должны **оставлять** электронный ключ, подключенным к компьютеру, в случае их отсутствия на рабочем месте.

6.11. В случае увольнения сотрудника или изменения его должностных обязанностей непосредственный руководитель **обязан** своевременно инициировать процедуру отключения (изменения) прав доступа данных сотрудников к ИР.

7. РАБОТА С СЕТЬЮ ИНТЕРНЕТ

7.1. Доступ сотрудников к сети Интернет предоставляется **только** в связи с необходимостью осуществления ими своих непосредственных должностных обязанностей.

7.2. Запрещается указывать аутентификационные данные (идентификатор доступа и пароль) для регистрации на web-сайтах, не имеющих непосредственного отношения к исполнению сотрудником должностных обязанностей (например, социальные сети, Интернет-магазинов и пр.) и/или на которых указанная информация будет доступна другим пользователям сайта (например, форумы).

7.3. Сотрудникам **запрещается** пользоваться службами мгновенных сообщений (ICQ, MSN Messenger Connect for Enterprises и т.п.), посещать сервисы бесплатной электронной почты, а также сайты, не имеющие отношения к выполнению должностных обязанностей.

7.4. Все действия сотрудников и сведения по работе в сети Интернет (посещаемые сайты,

объем отправленной и принятой информации и т.п.) сохраняются в специальных электронных журналах, которые периодически анализируются АИБ.

7.5. С целью недопущения заражения локальной вычислительной сети Организации компьютерными вирусами, сотрудникам **запрещается** самостоятельно загружать из сети Интернет какое-либо программное обеспечение и исполняемые файлы.

8. РАБОТА С УСТРОЙСТВАМИ ВВОДА-ВЫВОДА И СЪЕМНЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ

8.1. Устройства ввода-вывода

8.1.1. Устройства ввода-вывода, имеющие функции записи информации на носители, устанавливаются (подключаются) на рабочие компьютеры сотрудников Организации **в исключительных случаях**, если работа с такими устройствами вызвана необходимостью осуществления ими своих непосредственных должностных обязанностей. Для установки и подключения данных устройств оформляется Заявка, содержащая подробное обоснование необходимости такого доступа. Формулировки общего характера, такие как «в связи с производственной необходимостью», в качестве обоснования не принимаются.

8.1.2. Сотрудник, имеющий подключенное устройство ввода-вывода с функциями записи, **несет персональную ответственность** за его использование **только** для целей, указанных в Заявке.

8.2. Съемные носители информации

8.2.1. Подключение съемных носителей должно осуществляться только для непосредственной работы с ними. В случае отсутствия сотрудника на рабочем месте, все съемные носители информации должны быть извлечены и/или отсоединены сотрудником от компьютера. Оставлять указанные носители в неприсоединенном/неподключенном состоянии в местах открытого доступа и на столах без присмотра **запрещено**. Сотрудник должен убирать съемные носители в закрываемое на ключ место хранения или забирать с собой.

8.2.2. Сотрудники, допущенные к работе со съемными носителями информации, **обязаны** предъявлять их по требованию АИБ для проверки. Если съемный носитель не используется, подлежит замене (для ремонта) или подлежит сдаче, сотруднику необходимо также обратиться к АИБ для удаления всей информации, хранящейся на носителях. При увольнении или изменении должностных обязанностей, исполнение которых не требует использования съемных носителей информации, сотрудник обязан сдать съемный носитель сотруднику, осуществляющем выдачу носителей.

8.2.3. Самостоятельное приобретение съемного носителя для служебных целей возможно при разрешении вышестоящего руководителя и АИБ. Сотрудник должен **зарегистрировать** приобретенный съемный носитель у АИБ перед его использованием. Использование незарегистрированных в установленном порядке у АИБ съемных носителей информации **запрещено**.

8.2.4. Сотруднику запрещается передавать используемые съемные носители информации посторонним лицам или другим сотрудникам Организации без согласования непосредственного руководителя.

8.3. Съемные носители ключевой информации

8.3.1. Все съемные носители ключевой информации (далее - ключевые носители) сотрудник должен хранить в сейфе, запираемом на ключ шкафе, либо ином недоступном для посторонних лиц месте.

8.3.2. За каждым ключевым носителем приказом по Организации должен быть закреплен ответственный сотрудник. В случае необходимости выдачи ключевого носителя другим сотрудникам, ответственный сотрудник обязан согласовать передачу и/или списки сотрудников, имеющих право использовать данный ключевой носитель, с АИБ.

8.3.3. Сотруднику **запрещается** сообщать кому-либо пароли доступа (если таковые имеются) к используемым ключевым носителям, а также использовать записанный на ключевом носителе ключ для подписи каких-либо электронных документов (файлов) кроме тех, которые предусмотрены технологическим процессом в указанной системе защищенного документооборота.

8.3.4. В случае **компрометации**[1] криптографического ключа, т.е. обоснованного подозрения, что используемый ключ стал доступен постороннему лицу, пользователь обязан прекратить применение ключевого носителя, немедленно сообщить о факте компрометации (возможной компрометации) в подразделение информационной безопасности и непосредственному руководителю и действовать по их указанию.

8.3.5. При работе с ключевыми носителями должны, в том числе, соблюдаться требования, указанные в разделе 8.2 настоящей Политики ИБ.

9. РАБОТА С МОБИЛЬНЫМИ УСТРОЙСТВАМИ

9.1. Общие правила работы с мобильными устройствами

9.1.1. Сотрудникам **запрещается** подключение к локальной сети (компьютеру) личных мобильных устройств и их использование для работы с информацией ограниченного доступа.

9.1.2. Смартфоны и мобильные телефоны запрещается использовать для работы с конфиденциальной информацией.

9.1.3. **Запрещается** включать порты мобильного устройства, работающие на основе технологий беспроводной связи (IrDA, Wi-Fi, Bluetooth и WiMAX), подключать мобильные устройства к сетям сторонних юридических лиц и сетям общего пользования, в том числе Интернет. Запрещается оставлять карманные портативные компьютеры, сотовые телефоны и другие мобильные устройства на столах и прочих местах открытого доступа без присмотра.

9.1.4. В случае утери или кражи корпоративного мобильного устройства, сотрудник **обязан** немедленно письменно сообщить об этом своему непосредственному руководителю и АИБ, после чего составить и передать АИБ актуальный (т. е. на момент утери или кражи) перечень содержащейся в мобильном устройстве информации ограниченного доступа.

9.2. Особенности работы с ноутбуками

9.2.1. Запрещается передавать ноутбук в пользование другим сотрудникам. В случае необходимости передачи ноутбука другому сотруднику, необходимо обратиться к системному администратору для перенастройки ноутбука или согласовать с АИБ возможность использования ноутбука несколькими сотрудниками.

9.2.2. Ноутбуки запрещается оставлять без присмотра. При отсутствии на рабочем месте сотруднику следует убирать ноутбук в закрытое на ключ место хранения (сейф, металлический ящик), использовать специальный шнур безопасности с кодовым замком для предотвращения кражи оборудования или оставлять ноутбук под контроль других сотрудников подразделения, работающих в помещении.

9.2.3. В случае использования ноутбука за пределами здания Организации, сотрудник обязан использовать специальный кабель (шнур безопасности) для предотвращения кражи

[1] К событиям, связанным с компрометацией ключей, относятся потеря ключевого носителя (даже с последующим обнаружением), нарушение печати на сейфе (пенале) с ключевым носителем и т.п.

ноутбука, переносить ноутбук в специальной сумке, не оставлять ноутбук в автомобиле и в общественных местах; во время поездки на автомобиле располагать ноутбук в салоне автомобиля, принимая меры для предотвращения кражи через окно или дверь машины.

9.2.4. При использовании ноутбука для работы с информацией ограниченного доступа в общественных местах сотрудник обязан размещать его таким образом, чтобы предотвратить просмотр информации на экране сторонними лицами.

9.2.5. Во избежание потери информации, хранимой на ноутбуке, сотруднику следует по возможности осуществлять копирование информации в сетевые каталоги.

9.2.6. При работе с ноутбуками должны соблюдаться те же правила, что и при работе с персональными компьютерами, определенные в п. 5.1-5.5, 5.7 настоящей Политики ИБ.

9.2.7. При хранении на ноутбуке конфиденциальной информации необходимо обеспечить ее защиту от раскрытия в случае кражи устройства (например с помощью криптографического преобразования жесткого диска и защиты от загрузки с внешних носителей).

10. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. Контроль и мониторинг соблюдения настоящей Политики ИБ и требований информационной безопасности осуществляется АИБ в соответствии с установленными процедурами. АИБ имеет право проверять выполнение и требовать соблюдения сотрудниками настоящей Политики ИБ.

10.2. **По всем фактам** нарушения сотрудниками настоящей Политики ИБ и требований информационной безопасности АИБ **проводит детальное служебное расследование**, результаты которого доводятся до непосредственного руководителя сотрудника, а также до вышестоящего руководителя. По результатам расследования может быть принято решение о привлечении сотрудника, допустившего нарушение, к ответственности в соответствии с Правилами внутреннего трудового распорядка и Трудовым кодексом Российской Федерации. Порядок принятия такого решения определяется Трудовым кодексом РФ и внутренними нормативными актами Организации.