Государственное бюджетное учреждение города Москвы
Спортивно-Досуговый Центр «ФАВОРИТ»

№ 4/1 01.02.2021г.

П Р И К А З

Об обеспечении информационной безопасности в ГБУ «ФАВОРИТ»

На основании распоряжении префектуры Зеленоградского административного округа города Москвы № 610/7-ДСП от 22.11.2017г. «О результатах работы по развитию системы защиты информации и задачах на 2018 год»

ПРИКАЗЫВАЮ:

1. Утвердить «Политику информационной безопасности Государственного бюджетного учреждения города Москвы Спортивно-досугового Центра «ФАВОРИТ»;
2. Заместителям директора ГБУ «ФАВОРИТ»:

2.1. Руководствоваться в работе положениями Политики информационной безопасности информационных систем персональных данных для определения правил и обязанностей по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных в информационных системах персональных данных ГБУ «ФАВОРИТ»;

2.2. Ознакомить сотрудников с положениями Политики информационной безопасности информационных систем персональных данных, утвержденной настоящим приказом;

2.3. Требовать соблюдения специалистами учреждения положений Политики информационной безопасности при работе в информационных системах персональных данных Учреждения;

3. Контроль за исполнением приказа оставляю за собой.

Директор **И.С. Артемьева**

УТВЕРЖДАЮ
Директор ГБУ «ФАВОРИТ»
_____ И.С.Артемьева
«__1__» ___февраля___ 2021 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ ГОРОДА МОСКВЫ СПОРТИВНО-ДОСУГОВОГО ЦЕНТРА «ФАВОРИТ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Информация является ценным и жизненно важным ресурсом ГБУ «ФАВОРИТ» (далее – Учреждение). Настоящая политика информационной безопасности предусматривает принятие необходимых мер в целях защиты активов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Учреждении. Ответственность за соблюдение информационной безопасности несет каждый сотрудник Учреждения. Главные цели Учреждения не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей. В настоящей Политике под термином «сотрудник» понимаются все сотрудники Учреждения, включая лиц, работающих по гражданско-правовому договору на Учреждения независимо от вида и срока действия такого договора.

1.1. Цель и назначение Политики

Целями настоящей Политики являются:

• сохранение конфиденциальности значимых для Учреждения информационных ресурсов;

• обеспечение непрерывности доступа к информационным ресурсам Учреждения для поддержки деятельности;

• защита целостности деловой информации с целью поддержания возможности Учреждения по оказанию услуг высокого качества и принятию эффективных управленческих решений;

• повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Учреждения;

• определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Учреждении.

Руководители подразделений Учреждения должны обеспечить регулярный контроль за соблюдением положений настоящей Политики. Кроме того, должна быть организована периодическая проверка соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки Руководству.

1.2. Область применения настоящей Политики

Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации Учреждения. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации Учреждения, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей Политики.

Учреждению принадлежит вся деловая информация, любые документы и сведения, а также электронные документы, касающиеся ее деятельности, в том числе предпринимательской. В отношении указанных ресурсов вводится режим конфиденциальности, и все сотрудники Учреждения обязаны принимать меры к защите всех без исключения конфиденциальных данных.

2. ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ

2.1. Ответственность за информационные активы

В отношении всех собственных информационных активов Учреждения, активов, находящихся под контролем Учреждения, а также активов, используемых для получения доступа к инфраструктуре Учреждения, должна быть определена ответственность соответствующего сотрудника Учреждения. Эта ответственность указывается в трудовых договорах и в должностных инструкциях сотрудников Учреждения.

2.2. Контроль доступа к информационным системам

2.2.1. Общие положения

Все работы в пределах офисов Учреждения выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Учреждении.

Внос в здания и помещения Учреждения личных портативных компьютеров и внешних носителей информации (диски, дискеты, флеш-карты и т. п.), а

также вынос их за пределы Учреждения производится только при согласовании с руководителем или заместителем Учреждения. Все данные, составляющие тайну Учреждения и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы. Все портативные компьютеры Учреждения должны быть оснащены программным обеспечением по шифрованию жесткого диска.

В целях обеспечения санкционированного доступа к информационному ресурсу любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

В процессе своей работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.

2.2.2. Доступ третьих лиц к системам Учреждения

Каждый сотрудник обязан немедленно уведомить своего начальника обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети. Доступ третьих лиц к информационным системам Учреждения должен быть обусловлен производственной необходимостью. В связи с этим порядок доступа к информационным ресурсам Учреждения должен быть четко определен, контролируем и защищен.

2.2.3. Удаленный доступ

Пользователи получают право удаленного доступа к информационным ресурсам Учреждения с учетом их взаимоотношений с Учреждения.

Сотрудникам, использующим в работе портативные компьютеры Учреждения, может быть предоставлен удаленный доступ к сетевым ресурсам Учреждения в соответствии с правами в корпоративной информационной системе.

Сотрудникам, работающим за пределами Учреждения с использованием компьютера, не принадлежащего Учреждению, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ. Сотрудники и третьи лица, имеющие право удаленного доступа к

информационным ресурсам Учреждения, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Учреждения и к каким-либо другим сетям, не принадлежащим Учреждению. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Учреждения, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

2.2.4. Доступ к сети Интернет

Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила:

• сотрудникам Учреждения разрешается использовать сеть Интернет только в служебных целях;

• запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

• сотрудники Учреждения не должны использовать сеть Интернет для хранения корпоративных данных;

• работа сотрудников Учреждения с интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Учреждения в сеть Интернет;

• сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Учреждении;

• сотрудники Учреждения перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

• запрещен доступ в Интернет через сеть Учреждения для всех лиц, не являющихся сотрудниками Учреждения, включая членов семей сотрудников Учреждения.

2.3. Защита оборудования

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация Учреждения.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят авторизованные специалисты.

2.3.1. Аппаратное обеспечение

Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например принтеры и сканеры), аксессуары, коммуникационное оборудование (например факс-модемы, сетевые адаптеры и концентраторы) для целей настоящей Политики вместе именуется «компьютерное оборудование». Компьютерное оборудование, предоставленное Учреждением, является его собственностью и предназначено для использования исключительно в производственных целях.

Пользователи портативных компьютеров, содержащих информацию, составляющую информацию, не подлежащую разглашению Учреждения, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах, или обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства в случаях, когда данный компьютер не используется. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности как в офисе, так и по месту проживания. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например, в гостиницах, аэропортах, в офисах деловых партнеров и т. д., пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра.

Во время поездки в автомобиле портативный компьютер должен находиться в багажнике. На ночь его следует перенести из автомобиля в гостиничный номер.

Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавише и после выхода из режима экранной заставки. Для установки режимов защиты пользователь должен обратиться в службу технической поддержки. Данные не должны быть скомпрометированы в случае халатности или небрежности, приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

При записи какой-либо информации на носитель для передачи его контрагентам или партнерам по бизнесу необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

Карманные персональные компьютеры, а также мобильные телефоны, имеющие функцию электронной почты, и прочие переносные устройства не относятся к числу устройств, имеющих надежные механизмы защиты данных. В подобном устройстве не рекомендуется хранить конфиденциальную информацию.

Порты передачи данных, в том числе FD- и CD- дисководы в стационарных компьютерах сотрудников Учреждения блокируются за исключением тех случаев, когда сотрудником получено разрешение на запись информации у руководства.

2.3.2. Программное обеспечение

Все программное обеспечение, установленное на предоставленном Учреждением компьютерном оборудовании, является собственностью Учреждения и должно использоваться исключительно в производственных целях.

Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено руководителю Учреждения.

На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

• антивирусное программное обеспечение;

Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной руководителем Учреждения.

Сотрудники Учреждения не должны:

• блокировать антивирусное программное обеспечение;

• устанавливать другое антивирусное программное обеспечение;

• изменять настройки и конфигурацию антивирусного программного обеспечения.

2.4. Рекомендуемые правила пользования электронной почтой
Электронные сообщения (удаленные или неудаленные) могут быть доступны или получены для их использования в качестве доказательств в процессе судебного разбирательства. Поэтому содержание электронных сообщений должно строго соответствовать корпоративным стандартам в области деловой этики.

Использование электронной почты в личных целях допускается в случаях, когда получение/отправка сообщения не мешает работе других пользователей и не препятствует деятельности. Сотрудникам запрещается направлять партнерам конфиденциальную информацию Учреждения по электронной почте.

Сотрудникам Учреждения запрещается использовать публичные почтовые ящики электронной почты для осуществления какого-либо из видов корпоративной деятельности.

Сотрудники Учреждения для обмена документами с партнерами должны использовать только свой официальный адрес электронной почты. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свои имя и фамилию и тему сообщения.

Ниже перечислены недопустимые действия и случаи использования электронной почты:

• рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

• групповая рассылка всем пользователям Учреждения сообщений/писем;

• рассылка рекламных материалов, не связанных с деятельностью Учреждения;

• подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

• поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

• пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит корпоративным стандартам в области этики.

Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и они должны оформляться в соответствии с установленными в Учреждении процедурами документооборота.

Пересылка значительных объемов данных в одном сообщении может отрицательно повлиять на общий уровень доступности сетевой инфраструктуры Учреждения для других пользователей.

2.5. Сообщение об инцидентах информационной безопасности, реагирование и отчетность

Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте директору Учреждения.

Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов.

Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

• проинформировать своего непосредственного начальника;

• не пользоваться и не выключать зараженный компьютер;

• не подсоединять этот компьютер к компьютерной сети Учреждения до тех пор, пока на нем не будет произведено удаление обнаруженного вируса.

2.6. Управление сетью Сотрудникам Учреждения запрещается:

• нарушать информационную безопасность и работу сети Учреждения;

• сканировать порты или систему безопасности;

• контролировать работу сети с перехватом данных;

• получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;

• использовать любые программы, скрипты, команды или передавать сообщения в целях вмешаться в работу или отключить пользователя оконечного устройства;

• передавать информацию о сотрудниках или списки сотрудников Учреждения посторонним лицам;

• создавать, обновлять или распространять компьютерные вирусы и прочее разрушительное программное обеспечение.

2.6.1. Защита и сохранность данных Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

2.8. Разработка систем и управление внесением изменений Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, согласованны с руководителем Учреждения.