**УТВЕРЖДАЮ**
**Директор Государственного бюджетного учреждения города Москвы «Московская дирекция по развитию массового спорта» Департамента спорта города Москвы**

**_____ В.М.Владимиров**
**«___»_____ 2022 г.**

# ПОЛОЖЕНИЕ
## о защите информации и обеспечении информационной безопасности в Государственном бюджетном учреждении города Москвы «Московская дирекция по развитию массового спорта» Департамента спорта города Москвы

### 1. Общие положения

1.1.Настоящее Положение о защите информации и обеспечении информационной безопасности в Государственном бюджетном учреждение города Москвы «Московская дирекция по развитию массового спорта» Департамента спорта города Москвы (далее – Положение) определяет общий порядок получения, обработки, использования и защиты, определенной в соответствии с законодательством Российской Федерации информации ограниченного пользования, а также общие требования к информационным системам, содержащим такую информацию, в учреждении.

1.2.Настоящее Положение разработано в соответствие с федеральным законами и иными правовыми актами Российской Федерации, законами и иными правовыми актами города Москвы.

1.3.В целях настоящего Положения под информацией ограниченного пользования понимается образующаяся в процессе деятельности или поступившая в Государственное бюджетное учреждение города Москвы «Московская дирекция по развитию массового спорта» Департамента спорта города Москвы (далее – Учреждение) информация (сведения, сообщения, данные и т.п.), доступ к которой ограничен законодательством Российской Федерации, в том числе:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников

уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации;

- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

1.4.К информации ограниченного пользования не могут быть отнесены сведения, обязательные к раскрытию Учреждением в соответствии с законодательством Российской Федерации.

1.5.Настоящее Положение не распространяется на обработку обезличенных персональных данных, а также персональных данных, сделанных общедоступными субъектом персональных данных.

1.6.Учреждение организует обеспечение безопасности хранения, обработки и передачи по каналам связи информации, указанной в пункте 1.3 настоящего Положения.

1.7.Мероприятия по защите информации, указанной в пункте 1.3 настоящего Положения (далее - информация ограниченного пользования), осуществляются Учреждением во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.8.Обработка персональных данных в Учреждении осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

1.9.Объектами защиты информации в Учреждении являются:

- средства и системы информатизации и связи (средства вычислительной техники, локальная вычислительная сеть, средства и системы связи и передачи информации, средства звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи информации ограниченного пользования;

- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается информация ограниченного пользования;

- помещения (служебные кабинеты, актовые, конференц-залы и т.п.), специально предназначенные для проведения конфиденциальных мероприятий;

- помещения, специально предназначенные для хранения информации ограниченного пользования.

1.10. Ответственность за выполнение требований настоящего Положения

возлагается на должностное лицо, ответственное за защиту информации и обеспечение информационной безопасности в Учреждении (далее - ответственное должностное лицо), а также лиц, допущенных к обработке, передаче и хранению информации ограниченного пользования.

1.11. Непосредственное руководство мероприятиями по организации защиты информации ограниченного пользования в Учреждения осуществляет руководитель Учреждения.

## 2. Обеспечение защиты информации

2.1.Защита информации в Учреждении представляет собой комплекс организационных и технических мер и включает в себя обеспечение защиты информации ограниченного пользования от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

2.2.Для организации защиты информации ограниченного пользования руководитель Учреждения принимает следующие меры:

- утверждает перечень информации, подлежащей защите в Учреждении;
- назначает лицо, ответственное за организацию защиты информации и обеспечение информационной безопасности в Учреждении;
- утверждает списки работников Учреждения, которые в соответствии со своими должностными обязанностями допускаются к работе с информацией ограниченного пользования;
- определяет помещение, специально предназначенное для хранения информации ограниченного пользования, и обеспечивает его охрану;
- обеспечивает знакомство под подпись при приеме на работу в Учреждении работников, с перечнем информации, подлежащей защите в Учреждении;
- осуществляет контроль за обеспечением защиты информации ограниченного пользования;
- обеспечивает подключение к охранной сигнализации и передачу охранной организации на хранение помещения, специально предназначенного для хранения информации ограниченного пользования.

2.3.Мероприятия по защите информации ограниченного пользования в Учреждении осуществляются в соответствии с рекомендациями ГКУ «СМТК» Москомспорта.

## 3. Требования к информационной безопасности

3.1.Находящиеся в ведении Учреждения информационные системы и ресурсы, содержащие информацию ограниченного пользования, подлежат обязательной защите.

3.2.Информация ограниченного пользования должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической

защиты информации ограниченного пользования.

3.3.Уровень технической защиты информации ограниченного пользования, а также перечень необходимых мер защиты определяется в соответствии с рекомендациями ГКУ «ЦСТиСК» Москомспорта.

3.4.В целях обеспечения защиты информации ограниченного пользования работники Учреждения обязаны:

- хранить в тайне пароль (пароли), позволяющие получить доступ к информации ограниченного пользования;
- при служебной переписке использовать исключительно электронную почту в домене **mossport.ru;**
- поддерживать в актуальном состоянии антивирусное программное обеспечение, регулярно проводить его обновление;
- исключить физический доступ посторонних лиц к закрепленным за ним средствам обработки информации ограниченного пользования;
- неукоснительно выполнять предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и другого оборудования, установленного в помещении;
- немедленно вызывать ответственное должностное лицо и ставить в известность руководителя Учреждения в случае утери ключевого носителя электронно-цифровой подписи или при подозрении компрометации личных ключей и паролей, а также при обнаружении:
- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей при их наличии) на аппаратных средствах или иных фактов совершения в его отсутствие попыток несанкционированного доступа к рабочей станции;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств рабочей станции;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов рабочей станции или периферийных устройств (дисководов, принтеров и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на рабочей станции технических средств защиты;
- непредусмотренных формуляром рабочей станции отводов кабелей и подключенных устройств;
- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним рабочей станции в подразделении.
- передать Учреждению при прекращении или расторжении трудового договора имеющиеся в пользовании материальные носители информации, содержащие информацию ограниченного пользования.

3.5.Работникам Учреждения запрещается:

- использовать компоненты программного и аппаратного обеспечения Учреждения в неслужебных целях;
- самовольно вносить изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;
- для предотвращения заражения компьютеров вредоносным программным обеспечением, в том числе с полной потерей данных, запрещается открывать вложенные файлы и переходить по ссылкам из писем, полученных из недостоверных источников;
- осуществлять обработку информации ограниченного пользования в присутствии не допущенных к данной информации лиц;
- записывать и хранить информацию ограниченного пользования на неучтенных носителях информации;
- оставлять включенной без присмотра свою рабочую станцию, не активизировав средства защиты от несанкционированного допуска (временную блокировку экрана и клавиатуры);
- передавать кому-либо свой персональный носитель электронно-цифровой подписи (кроме руководителя Учреждения и руководителя структурного подразделения Учреждения; делать неучтенные копии носителя электронно-цифровой подписи (на любой другой носитель) и вносить какие-либо изменения в носитель электронно-цифровой подписи;
- использовать свой персональный носитель электронно-цифровой подписи для формирования цифровой подписи любых электронных документов, кроме регламентированных технологическим процессом на его рабочем месте;
- оставлять без личного присмотра на рабочем месте или где бы то ни было свой персональный носитель электронно-цифровой подписи, машинные носители и распечатки, содержащие информацию ограниченного пользования;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок необходимо ставить в известность ответственное должностное лицо.

3.6.Допускается использование только учтенные носители информации ограниченного пользования, которые подвергаются регулярной ревизии и контролю.

3.7.При использовании работниками Учреждения носителей информации ограниченного пользования необходимо:

- использовать носители информации ограниченного пользования исключительно для выполнения своих служебных обязанностей;
- обеспечивать физическую безопасность носителей информации ограниченного пользования всеми разумными способами;
- извещать ответственное должностное лицо и руководителя Учреждения о фактах утраты (кражи) носителей информации ограниченного пользования.

3.8.При использовании носителей информации ограниченного пользования запрещено:

- использовать носители информации ограниченного пользования в личных целях;

- передавать носители информации ограниченного пользования другим лицам (за исключением директора Учреждения и ответственного должностного лица);

- хранить носители информации ограниченного пользования вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить носители информации ограниченного пользования из служебных помещений для работы с ними без согласования руководителя Учреждения.

3.9.Любое взаимодействие (обработка, прием/передача информации) инициированное работником Учреждения между информационной системой, содержащей информацию ограниченного пользования и неучтенными (личными) носителями информации, рассматривается как несанкционированное.

3.10. В случае выявления фактов несанкционированного и/или нецелевого применения носителей информации ограниченного пользования инициализируется служебная проверка, проводимая комиссией, состав которой определяется руководителем Учреждения.

3.11. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю Учреждения для принятия мер согласно локальным нормативным актам и законодательству Российской Федерации.

3.12. Информация, хранящаяся на носителях информации ограниченного пользования, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.

3.13. В случае увольнения или перевода работника в другое структурное подразделение Учреждения, предоставленные носители информации ограниченного пользования изымаются.

**4. Заключительные положения**

4.1.В целях обеспечения защиты информации и обеспечения информационной безопасности Учреждение имеет право привлекать к проведению работ по технической защите информации в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

4.2.При проведении Учреждением совместных работ с физическими лицами, юридическими лицами, органами государственной власти, органами местного самоуправления, связанных с информацией ограниченного пользования, должна быть обеспечена техническая защита информации ограниченного пользования независимо от места проведения работ.

4.3.Публикация на официальном сайте Учреждения в информационно-телекоммуникационной сети «Интернет» информации, содержащей персональные данные, осуществляется в соответствии с законодательством Российской Федерации.

4.4.Публикация на официальном сайте Учреждения в информационно-

телекоммуникационной сети «Интернет» информации, содержащей сведения, составляющие государственную и иную охраняемую законодательством Российской Федерации тайну, сведения конфиденциального характера, а также информации ограниченного пользования не допускается.

4.5.Учреждение имеет право пройти добровольную аттестацию на соответствие требованиям по технической защите информации ограниченного пользования в порядке, установленном законодательством Российской Федерации.

4.6.Настоящее Положение обязательно для исполнения всеми работниками Учреждения, которые должны быть ознакомлены с ним под подпись.

4.7.Нарушение требований к работе с информацией ограниченного пользования, влечет материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации и локальными актами Учреждения.

4.8.Настоящее Положение вступает в силу после его утверждения руководителем Учреждения.

---