Утверждаю
директор МБУДО ДДТ
_____ В.Коршикова

ИНСТРУКЦИЯ
пользователя по обеспечению информационной безопасности автоматизированного рабочего места, выделенного для обработки конфиденциальной информации (персональных данных) в МБУДО ДДТ

В Инструкции пользователя по обеспечению информационной безопасности при работе с базами данных МБУДО Дома детского творчества (далее – учреждение) использованы следующие термины и определения:

1. База данных (далее - БД) - централизованное хранилище информации, оптимизированное для многопользовательского доступа и работающее под управлением системы управления базами данных (далее - СУБД).

2.Комплекс программных средств (далее - КПС) - система или приложение, использующее непосредственный доступ к БД.

3.Идентификатор (учетное имя или login) - присвоенная пользователю индивидуально буквенно-числовая последовательность, используемая для идентификации пользователя при установлении доступа к БД и позволяющая однозначно определять работу конкретного пользователя в БД.

4. Пароль - секретная персональная последовательность символов, известная только пользователю, которая используется совместно с идентификатором для доступа в БД и позволяет подтвердить, что доступ к БД осуществляет именно конкретный пользователь.

5. Пользователи - должностные лица МБУДО ДДТ, педагоги дополнительного образования а также все другие лица и учреждении, работающие с БД

6.Администратор БД - должностное лицо МБУДО ДДТ , уполномоченные для выполнения административных функций и обеспечивающие функционирование БД и ее безопасность соответственно.

7.Локально-вычислительная сеть (далее - ЛВС) - группа компьютеров, а также периферийное оборудование, объединенные одним или несколькими автономными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

8. Политика информационной безопасности - комплекс организационно-технических мероприятий, правил и условий использования информационных систем учреждения, определяющих нормальное функционирование систем и обеспечение безопасности информации, обрабатываемой в учреждении

Настоящий документ разработан на основе Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, с целью совершенствования методического обеспечения деятельности в данной области государственных и муниципальных органов, юридических и физических лиц, организующих и (или) осуществляющих обработку персональных данных (ПДн), определяющих цели и содержание обработки ПДн (операторов), а также заказчиков и разработчиков информационных систем персональных данных (ИСПДн) при решении ими задач по обеспечению безопасности ПДн.

Общие положения по организации доступа к конфиденциальной информации в МБУДО ДДТ.

1.Инструкция пользователя определяет комплекс организационно - технических мероприятий по обеспечению безопасности конфиденциальной информации, хранящейся на компьютерах школы в БД и обрабатываемой с помощью средств вычислительной техники в учреждении.

2.Инструкция пользователя является частью политики информационной безопасности , предназначена для обеспечения эффективной организации и управления доступом пользователей к конфиденциальной информации, хранящейся на компьютерах школы и в БД учреждения, и содержит требования по обеспечению информационной

безопасности учреждения в части выполнения операций со кофиденциальной информацией и по организации и управлению доступом к БД.

3. Требования Инструкции пользователя обязательны для выполнения всеми пользователями, которым предоставляется доступ к конфиденциальной информации учреждения.

4.Доступ к к конфиденциальной информации учреждения предоставляется исключительно пользователям, утверждённым приказом администрации учреждения через предоставленный системным администратором ДДТ пароль.

5.Решение задач, связанных с организацией и управлением доступом должностных лиц школы к конфиденциальной информации, осуществляется системным администратором школы.

При возникновении ситуаций, не включенных в положения настоящей Инструкции пользователя, решение принимает системный администратор.

6.Для доступа к БД школы у каждого пользователя БД должен иметь свой уникальный идентификатор и пароль доступа к БД.

7.Доступ к БД школы может быть предоставлен с любого компьютера административной локальной сети.

8.Доступ к БД предоставляется пользователям на срок действия их трудовых отношений и исполнения служебных обязанностей в МБУДО ДДТ

Обязанности и ответственность пользователей автоматизированных рабочих мест, выделенных для обработки конфиденциальной информации.

1.Перед началом первой работы с конфиденциальной информацией пользователь обязан изучить Инструкцию пользователя и ознакомиться с ответственностью за выполнение требований Инструкции пользователя при работе с конфиденциальной информацией под роспись.

2.Пользователю запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа к конфиденциальной информации другим лицам. Запрещается хранение пароля в общедоступных местах, позволяющих другим лицам получить информацию о пароле.

3.Пользователь конфиденциальной информации обязан обеспечивать правильность ввода и коррекции данных, за которые он отвечает.

4.Пользователь обязан закрывать соединение с БД учреждения на время своего отсутствия у рабочей станции БД или вообще выходить по доступу к ресурсам компьютера с конфидициальными данными из своего идентификатора (*например, teacher, secret, adminic и т.п., через Пуск_ Завершить сеанс Имя идентификатора*).

5.В случае выявления инцидентов с доступам к ресурсам компьютера с конфиденциальными данными (фактов несанкционированного доступа посторонними людьми, людьми без допуска к конфиденциальным данным) пользователь обязан незамедлительно сообщить об этом системному администратору ДДТ.

6.В случае выявления инцидентов с доступом к БД учреждения (фактов несанкционированного доступа к БД, блокировки доступа, утери или компрометации пароля и т.п.) пользователь обязан незамедлительно сообщить об этом администратору БД.

7.Установку и конфигурирование программного обеспечения на компьютерах с доступом к конфиденциальным данным школы выполняет системный администратор или администратор БД школы. Пользователям данных рабочих мест запрещается самостоятельно устанавливать какое-либо программное обеспечение.

8.Пользователю запрещается использовать информацию, полученную в результате доступа к конфиденциальным данным школы, в целях, не предусмотренных его функциональными обязанностями и технологическими схемами. Он не вправе разглашать, использовать в личных целях, либо передавать третьим лицам, в том числе государственным органам, конфиденциальную информацию, за исключением случаев, установленных законами Российской Федерации.

9.При нарушениях правил, связанных с информационной безопасностью, пользователь несет ответственность, установленную действующим законодательством Российской Федерации.

10. Пользователь несет ответственность за все действия, совершенные от имени его идентификатора, учетной записи или логина, если не доказан факт несанкционированного использования таковых.