САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ КУЛЬТУРЫ

МИНИСТЕРСТВО КУЛЬТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Самарский государственный институт культуры» (СГИК)

ПРИКАЗ

От 26. 08. 2024 г № 119

г. Самара

Об утверждении Политики информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Самарский государственный институт культуры»

В соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», с целью обеспечения информационной безопасности в федеральном государственном бюджетном образовательном учреждении высшего образования «Самарский государственный институт культуры» (далее - СГИК), **приказываю:**

1. Утвердить и ввести в действие Политику информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Самарский государственный институт культуры» (Приложение).
2. Начальнику медиацентра (М.Е. Драпеза) обеспечить размещение приказа на официальном сайте СГИК в подразделе «Документы», раздела «Сведения об образовательной организации» в течение 10 дней с момента издания приказа.
3. Контроль за исполнением приказа оставляю за собой.

Ректор О. С. Наумова

Приложение
к приказу ректора Самарского
государственного института культуры
от «26» 08 20 24 г. № 119

Политика информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Самарский государственный институт культуры»

1. Общие положения

1.1. Настоящая Политика определяет цели и принципы обеспечения информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Самарского государственного института культуры» (далее - СГИК, Институт).

1.2. Политика обязательна для исполнения всеми работниками СГИК.

1.3. Настоящая Политика не распространяется на организацию и порядок защиты информации, составляющей государственную тайну.

1.4. Настоящая Политика может изменяться в одностороннем порядке. Актуальная версия Политики размещена на официальном сайте СГИК samgik.ru.

2. Основные понятия и определения

2.1. Конфиденциальность - состояние информации, при котором доступ к ней осуществляют только те субъекты, которые имеют на это право.

2.2. Целостность - состояние информации, при котором изменять информацию могут только те субъекты, которые имеют на это право.

2.3. Доступность - состояние информации, при котором субъекты, имеющие право доступа к информации, могут осуществлять его беспрепятственно.

3. Основные цели и задачи

3.1. Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности.

3.2. Целями обеспечения информационной безопасности являются:

- предотвращение и минимизация ущерба от реализации угроз информационной безопасности СГИК:

- обеспечение непрерывности основных бизнес-процессов СГИК.

3.3. Основными задачами деятельности по обеспечению информационной безопасности СГИК являются:

- соответствие требованиям законодательства Российской Федерации в области обеспечения информационной безопасности;

- разработка и актуализация модели угроз безопасности информации;

- использование современных методов защиты информации;

- разработка и актуализация положений, регламентов, инструкций по обеспечению информационной безопасности СГИК;

- реализация организационных и технических мероприятий по защите конфиденциальной информации;

- контроль за выполнением требований по обеспечению информационной безопасности СГИК.

4. Категории конфиденциальной информации

Определение категорий конфиденциальной информации, порядок отнесения сведений к конфиденциальной информации СГИК, а также обработки и защиты, определение ответственности за лицами, имеющими к ним доступ, закрепляются локальными актами СГИК.

Разовый либо постоянный допуски к конфиденциальной информации оформляются в соответствии с принятым в СГИК порядке (Служебная записка на имя начальника отдела информационных технологий).

5. Основные принципы деятельности в сфере обеспечения информационной безопасности

Обработка информации в Институте производится с соблюдением следующих принципов:

- соблюдение конфиденциальности сведений, признанных СГИК подлежащими защите, а также целостности и доступности данных сведений;

- дифференцированный подход к обеспечению безопасности информации;

- ответственности и отчетности СГИК перед гражданином (в том числе перед работником Института) за обработку сведений, содержащих его персональные данные;

- учет и контроль всех этапов автоматизированной и неавтоматизированной обработки конфиденциальной информации;

- осведомленности работников Института, осуществляющих обработку конфиденциальной информации в вопросах информационной безопасности;

- персональная ответственность работников Института за выполнение норм информационной безопасности;

- использование принципа минимальных привилегий: доступ к конфиденциальной информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.

6. Иерархия документов, касающихся информационной безопасности в СГИК

6.1. Иерархия документов:

6.1.1. Политика информационной безопасности СГИК;

6.1.2. Положения, политики, касающиеся информационной безопасности, в том числе различных категорий конфиденциальной информации;

6.1.3. Регламенты, инструкции, конкретизирующие вопросы информационной безопасности в отдельных областях.

6.2. Актуальный перечень документов согласно иерархии документов (п. 6.1.) составляется (корректируется) отделом информационных технологий.

7. Ответственность и контроль

7.1. Общий контроль и координацию работ по обеспечению информационной безопасности начальник отдела информационных технологий

7.2. Текущий контроль за обеспечением информационной безопасности в СГИК осуществляет отдел информационных технологий.

Отдел информационной технологий несет ответственность за контроль исполнения данной политики.

7.3. Нарушение требований Политики, локальных нормативных актов по обеспечению информационной безопасности влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, локальными нормативными актами, договорами, заключенными между Институтом и работниками (обучающимися).

7.4. Руководители структурных подразделений несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях, обязаны незамедлительно сообщать в отдел информационных технологий о всех инцидентах, связанных с нарушениями требований информационной безопасности.

8. Заключительное положение

8.1. Настоящая Политика вступает в юридическую силу с момента утверждения приказом ректора Института и действует до дня замены новой (отмены в установленном порядке).

8.2. Дополнения и изменения в настоящую Политику принимаются и утверждаются приказом ректора Института.