Автономная некоммерческая общеобразовательная организация

ТОЛЬЯТТИНСКАЯ КЛАССИЧЕСКАЯ
ГИМНАЗИЯ ВО ИМЯ ВСЕХ РУССКИХ СВЯТЫХ
(ПРАВОСЛАВНАЯ КЛАССИЧЕСКАЯ ГИМНАЗИЯ)

г.о. Тольятти (Ставрополь-на-Волге)

СОГЛАСОВАНО
Исполнительный директор
_____ Ю. Г. Лескина
«01» сентября 2025 г.

УТВЕРЖДАЮ
Директор _____
протоиерей Дмитрий Лескин
«01» сентября 2025 г.

Политика информационной безопасности

1. Область применения

1.1. Настоящая Политика информационной безопасности (далее – Политика), применяемая в Тольяттинской Классической гимназии «Во имя всех Русских святых» (далее – Учреждение), является локальным нормативным актом, устанавливающим ключевые цели, задачи и основополагающие принципы организации системы обеспечения информационной безопасности.

1.2. Данная Политика определяет основные направления деятельности в сфере информационной безопасности, устанавливает комплекс правил, требований и базовых принципов, которыми руководствуется Учреждение в своей работе.

1.3. Положения настоящей Политики являются обязательными для исполнения всеми работниками Учреждения.

1.4. Политика создана в полном соответствии с действующим законодательством Российской Федерации в сфере обеспечения защиты и безопасности информации.

2. Термины и определения

2.1. В рамках настоящей Политики используются следующие термины:

- **актив** – любой объект, представляющий ценность для Учреждения;
- **анализ риска** – систематическая работа с информацией для выявления источников и оценки уровня риска;
- **доступность** – обеспечение санкционированного доступа к информации и связанным с ней ресурсам уполномоченных пользователей при необходимости;
- **защита информации** – обеспечение конфиденциальности, целостности и доступности информационных ресурсов;
- **конфиденциальность** – ограничение доступа к информации исключительно для уполномоченных лиц;
- **оценка риска** – комплексный процесс анализа и определения значимости рисков;
- **риск** – сочетание вероятности наступления события и его последствий;
- **средства обработки информации** – любые системы, сервисы или инфраструктуры обработки данных, а также их физическое расположение;
- **средство управления** – инструменты контроля рисков, включающие политику, процедуры, руководящие указания, практики или организационные структуры;
- **третья сторона** – физическое или юридическое лицо, независимое от участвующих сторон в рассматриваемом вопросе;

- **угроза** – потенциальный источник нежелательного события, способного нанести ущерб системе или Учреждению;
- **целостность** – гарантия достоверности и полноты информации и методов её обработки.

3. Общие положения

3.1. Политика разработана для достижения следующих целей:

- информирование сотрудников Учреждения о мерах обеспечения информационной безопасности;
- обеспечение соответствия деятельности Учреждения законодательным требованиям в сфере информационной безопасности, включая защиту персональных данных;
- защита интересов Учреждения при обеспечении надлежащего уровня безопасности информационных активов.

3.2. Положения Политики распространяются на всю деятельность Учреждения, включая всех участников разработки и внедрения информационных систем.

3.3. Требования Политики могут быть применены к организациям, взаимодействующим с Учреждением в рамках информационного обмена.

3.4. Информационная безопасность определяется как состояние защищённости информационных ресурсов от несанкционированного доступа, утечки, модификации, уничтожения или блокирования.

3.5. Политика служит основой для:

- создания систем защиты информации;
- организации защищённого документооборота;
- разработки нормативных документов в сфере информационной безопасности;

- обеспечения прав на доступ к информации.

4. Цели политики информационной безопасности

4.1. Ключевые цели политики:

- управление рисками информационной безопасности;
- обеспечение конфиденциальности персональных данных;
- защита целостности информационных ресурсов;
- соответствие стандартам безопасности информационных систем.

5. Принципы информационной безопасности

5.1. Система строится на следующих принципах:

- принятие и управление рисками информационной безопасности;
- обязательная информированность персонала о требованиях безопасности;
- обеспечение необходимого финансирования мер защиты;
- предотвращение злоупотреблений в информационных системах;
- регулярный мониторинг состояния информационной безопасности;
- недопущение нарушений законодательства.

6. Заключительные положения

6.1. Ответственность за нарушение требований законодательства РФ и внутренних нормативных документов определяется в соответствии с действующим законодательством.

6.2. Политика вступает в силу с момента утверждения и действует до принятия новой редакции.

6.3. Любые изменения и дополнения к Политике утверждаются директором Тольяттинской Классической гимназии «Во имя всех Русских святых».