# Политика информационной безопасности

## 1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее - Политика) определяет основные принципы и требования к обеспечению информационной безопасности Муниципалитета [Населенного пункта] (далее - Муниципалитет).

1.2. Политика разработана в соответствии с **международными стандартами серии ISO/IEC 27000**, а также с учетом следующих нормативно-правовых актов (НПА):

* **ФЗ № 149-ФЗ "Об информации, информационных технологиях и о защите информации"**
* **ФЗ № 152-ФЗ "О персональных данных"**
* **ФЗ № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"**
* **Постановления Правительства РФ по защите информации**

## 2. Область применения

2.1. Политика распространяется на:

* Всех сотрудников Муниципалитета
* Всех подрядчиков и третьих лиц, имеющих доступ к информационным ресурсам Муниципалитета
* Все процессы и операции, связанные с обработкой информации
* Информационные системы и ресурсы, используемые для оказания муниципальных услуг
* Процессы электронного документооборота
* Все муниципальные информационные системы и сервисы

2.2. Действие Политики распространяется на все виды информации, обрабатываемой в муниципальном образовании, включая:

* Персональные данные граждан
* Служебную информацию
* Конфиденциальные данные
* Открытую информацию официального характера

2.3. Политика является обязательным к исполнению документом для всех структурных подразделений Администрации и подведомственных учреждений.

2.4. Требования Политики имеют приоритетный характер над локальными нормативными актами муниципальных учреждений в части обеспечения информационной безопасности.

## 3. Определения

3.1. **Информационная безопасность** - защита информации от несанкционированного доступа, использования, распространения, изменения или уничтожения, включая меры по обеспечению конфиденциальности, целостности и доступности информации, а также защиту персональных данных граждан.

3.2. **Конфиденциальная информация** - любые данные, доступ к которым ограничен в соответствии с законодательством или внутренними документами Муниципалитета.

3.3 **Персональные данные -** любая информация, которая прямо или косвенно относится к конкретному физическому лицу.

## 4. Цели и задачи

4.1. Основными целями являются:

* Обеспечение конфиденциальности, целостности и доступности информации
* Защита персональных данных сотрудников и клиентов
* Предотвращение утечек конфиденциальной информации
* Соблюдение требований законодательства
* Защита критической информационной инфраструктуры

4.2. Основные задачи:

* Внедрение системы управления информационной безопасностью
* Регулярный мониторинг и оценка рисков
* Регулярное проведение обучения и повышения квалификации сотрудников в области информационной безопасности

## 5. Метрики

5.1. Основными метриками являются:

* % времени бесперебойной работы АСУГТ (>99,5%) (Ответственный - главный ИТ-специалист)
* Время восстановления после сбоя ЭПГ (<1 ч) (Ответственный - ответственный за поддержку портала)
* Количество утечек (0 случаев в год) (Ответственный - специалист по защите ПДн)
* Количество устраненных уязвимостей (>90%) (Ответственный - администратор безопасности)

5.2 Обоснование метрик

* Если метрика доступности АСУ ГТ >99,5% → транспортная система работает стабильно
* Если среднее время восстановления после сбоя <1 часа → граждане могут оперативно подать обращения
* Если количество утечек = 0 → персональные данные защищены
* Если устранено >90% уязвимостей → снижена вероятность успешных атак

5.3 Прогноз метрик

* Через 1 год: Снижение инцидентов ИБ на 30%.
* Через 3 года: Устранение критических уязвимостей, время восстановления ЭПГ ≤ 30 минут.
* График: Экспоненциальное снижение числа инцидентов при росте зрелости процессов.

## 6. Принципы обеспечения информационной безопасности

6.1. Непрерывность защиты: процесс защиты информации должен продолжаться непрерывно на протяжении существования информации  
6.2. Комплексность мер безопасности: меры безопасности должны обеспечивать защиту информации от всех типов атак, которые могут быть применены к информации  
6.3. Ответственность всех сотрудников  
6.4. Соответствие законодательным требованиям

## 7. Обязанности и ответственность

7.1. Руководство Муниципалитета:

* Обеспечивает выделение необходимых ресурсов
* Поддерживает и контролирует выполнение Политики
* Принимает решения по вопросам информационной безопасности
* Обеспечивает разработку и актуализацию нормативных документов по ИБ

7.2. Сотрудники:

* Соблюдают требования Политики
* Проходят регулярное обучение по защите персональных данных граждан
* Сообщают о выявленных угрозах
* Поддерживают установленный уровень квалификации в области ИБ

## 8. Основные меры безопасности

8.1. Технические меры:

* Использование антивирусного ПО
* Шифрование данных
* Регулярное обновление программного обеспечения
* Внедрение систем обнаружения и предотвращения вторжений (IDS/IPS)
* Регулярное резервное копирование данных
* Защита от DDoS-атак

8.2. Организационные меры:

* Разграничение доступа
* Контроль физического доступа
* Управление паролями
* Назначение ответственного лица, который будет контролировать соблюдение политики
* Проведение регулярных проверок соблюдения политик безопасности
* Разработка и актуализация документации по ИБ

8.3. Физическая безопасность:

* Контроль доступа в серверные
* Видеонаблюдение

## 9. Управление инцидентами

9.1 Критические события и риски:

* Сбой АСУТ, ведущий к остановке транспорта.
* Утечка данных из ЭПГ.
* DDoS-атака на ЭПГ.
* Несанкционированный доступ к системам управления.
* Операционные потери из-за простоя транспорта.
* Репутационный ущерб при утечке данных.
* Нарушение законодательства (штрафы до 6 млн руб. по ст. 13.11 КоАП).

9.1. Порядок обнаружения:

* Мониторинг событий безопасности
* Анализ журналов событий
* Обработка сообщений о подозрительной активности

9.2. Порядок реагирования:

* Оценка серьезности инцидента
* Локализация угрозы
* Минимизация ущерба
* Восстановление нормальной работы

## 10. Контроль и мониторинг

10.1. Регулярные проверки:

* Аудит безопасности
* Тестирование на проникновение
* Проверка соответствия требованиям

10.2. Отчетность:

* Ежемесячные отчеты о состоянии безопасности
* Квартальные отчеты о выявленных уязвимостях
* Годовые отчеты о выполнении Политики

## 11. Заключительные положения

11.1. Политика утверждается руководством Организации  
11.2. Документ подлежит пересмотру не реже одного раза в год  
11.3. Все изменения согласовываются с отделом информационной безопасности и утверждаются руководителем муниципалитета

Дата утверждения: \_\_\_\_\_\_\_\_\_

Руководитель организации: \_\_\_\_\_\_\_\_\_