ПРИЛОЖЕНИЕ 1 к
приказу № ___ от 17.03.25
П03-00201

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МУНИЦИПАЛЬНОГО УНИТАРНОГО ПРЕДПРИЯТИЯ Г. АСТРАХАНИ «АСТРВОДОКАНАЛ»

1. Настоящая политика определяет цели и принципы обеспечения информационной безопасности в муниципальном унитарном предприятии г. Астрахани «Астрводоканал» (далее - Предприятие).
2. Политика обязательна для исполнения всеми сотрудниками, а также лицами, работающими с конфиденциальной информацией, принадлежащей Предприятию, в рамках заключенных договоров.
3. Целями обеспечения информационной безопасности являются минимизация ущерба от реализации угроз информационной безопасности.
4. Основные задачи деятельности по обеспечению информационной безопасности Предприятия:
   - выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
   - предотвращение инцидентов информационной безопасности;
   - исключение либо минимизация выявленных угроз.
5. На Предприятии обрабатываются следующие категории информации ограниченного доступа (конфиденциальная информация):
   - Персональные данные работников Предприятия.
   - Персональные данные практикантов, соискателей и иных лиц.
   - Персональные данные абонентов/контрагентов и заявителей (в бумажном и электронном виде), к которым Предприятие получает доступ в рамках осуществления своей деятельности.

   Порядок обработки и защиты каждой категории сведений, закрепление ответственности за лицами, имеющими к ним доступ, в том числе санкции за невыполнение норм безопасности, регулирующих обработку и защиту конфиденциальной информации, закрепляются соответствующими локальными нормативными актами.
6. Обработка информации на Предприятии производится с соблюдением следующих принципов:
   - соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами;
   - дифференцированный подход к обеспечению безопасности информации на основе ее классификации по степени ущерба от нарушений свойств безопасности;
   - ответственности и отчетности Предприятия перед гражданином за обработку сведений, содержащих его персональные данные.
7. Доступ к конфиденциальной информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме. При этом разовый либо постоянный допуски к

конфиденциальной информации оформляются приказом генерального директора Предприятия.

8. Стратегия Предприятия в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Предприятия, до специализированных мер информационной безопасности.
9. Меры защиты информации, выбираемые Предприятием, внедряются по результатам проведения оценки рисков информационной безопасности. Оценка рисков информационной безопасности проводится периодически, а также в случае значительных изменений в структуре и бизнес-процессах Предприятия. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.
10. Требования настоящей политики могут уточняться и дополняться другими внутренними нормативными документами Предприятия и при этом должны не противоречить ей.
11. Порядок обработки и защиты конфиденциальной информации, закрепление ответственности за лицами, имеющими к ней доступ, в том числе санкции за невыполнение требований норм, регулирующих обработку и защиту конфиденциальной информации, закрепляются соответствующими локальными нормативными актами.
12. Администратор информационной безопасности обязан ознакомить работника с настоящей Политикой под подпись после заключения трудового договора.
13. Неисполнение или некачественное исполнение сотрудниками Предприятия и пользователями информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным административных, дисциплинарных и прочих мер воздействия, степень которых определяется установленным в Предприятии порядком либо требованиями действующего законодательства.