

ПОЛИТИКА ГБУ ЛО «СББЖ ВОЛОСОВСКОГО РАЙОНА» В ОБЛАСТИ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ

(на основании Политики обработки и защиты ПДн, ред. от 05.05.2026, утв. приказом № 35-п,

Цель политики

- Обеспечение безопасности информационных ресурсов, операций, персонала, инфраструктуры, сетей передачи данных и носителей информации.

Предотвращение и минимизация потерь ГБУ ЛО «СББЖ Волосовского района» от:

- Утечек конфиденциальной информации (в том числе служебной, ветеринарной, персональных данных);
- Использования недостоверной, искаженной информации;
- Нарушения процессов обработки информации;
- Обеспечение выполнения и контроль соблюдения требований законодательства и локальных нормативных актов в области защиты информации (в том числе о персональных данных и служебной тайне);
- Повышение осведомленности персонала в вопросах, относящихся к информационной безопасности (инструктажи, обучение).

Наши обязательства

- Строго соблюдать требования Федерального закона № 152-ФЗ «О персональных данных» и иных нормативных правовых актов.
- При сборе персональных данных предоставлять субъекту по его запросу полную информацию об обработке.
- Обеспечивать запись, систематизацию, накопление, хранение, уточнение и извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории РФ.
- Принимать правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения.
- Уточнять, блокировать или уничтожать персональные данные, если они неполны, устарели, неточны, получены незаконно или не являются необходимыми для заявленной цели.
- Прекращать обработку при отзыве согласия субъекта (за исключением случаев, предусмотренных законом).
- В случае инцидента с персональными данными уведомлять Роскомнадзор в течение 24 часов, а в течение 72 часов предоставлять результаты внутреннего расследования.

Направления деятельности

- Создание, поддержка и развитие системы защиты информации, соответствующей требованиям законодательства РФ, задачам ветеринарной безопасности и лучшим практикам в государственных учреждениях;
- Прогнозирование, предупреждение, выявление, противодействие и нейтрализация внешних и внутренних угроз информационной безопасности, а также минимизация ущерба от их воздействия;
- Реализация комплекса мероприятий по обеспечению безопасности информационных систем (в том числе систем учета ветеринарных операций), персонала, инфраструктуры, сетей передачи данных и носителей информации;
- Несанкционированного доступа к информационным системам и ресурсам.
- Внутренний контроль и аудит соответствия обработки персональных данных установленным требованиям.
- Ознакомление всех сотрудников, имеющих доступ к персональным данным, с законодательством и внутренними документами.

Наши принципы

- Законность.** Система защиты информации должна соответствовать требованиям законодательства Российской Федерации.
- Целевая направленность.** Меры защиты информации соответствуют целям и задачам Учреждения, установленным Уставом (обеспечение ветеринарной безопасности, защита здоровья людей и животных).
- Минимизация полномочий.** Доступ к информационным ресурсам и технологиям должен быть ограничен, обоснован и предоставляться исключительно для выполнения служебных обязанностей.
- Достоверность.** Принимаются меры для обеспечения точности и актуальности персональных данных.
- Системность.** Организационные меры и технические средства должны разрабатываться и применяться в рамках единой системы защиты, учитывающей все способы реализации актуальных угроз и не содержащей слабых мест на стыке отдельных ее компонентов.
- Непрерывность.** Процессы, связанные с обеспечением информационной безопасности, должны выполняться на всех этапах жизненного цикла информации - от создания до уничтожения. Каждый работник на своем уровне должен принимать участие в этих процессах.
- Контроль.** Информационные ресурсы и средства коммуникаций должны предусматривать механизмы контроля порядка обращения с конфиденциальной информацией.
- Прозрачность.** Субъекты персональных данных информируются об обработке и имеют возможность реализовать свои права, включая доступ, уточнение, блокирование и отзыв согласия.
- Постоянное совершенствование.** Система защиты информации должна развиваться и совершенствоваться в соответствии с появлением новых угроз, изменениями в информационных системах и нормативных актах, опираться на достигнутые результаты и лучшие практики.

Павлов А.Н., Начальник
ГБУ ЛО «СББЖ Волосовского района»

