Приложение 1

УТВЕРЖДЕНО
приказом ГБСУСОССЗН
«Ливенский дом социального
обслуживания»
от 09.01.2023 г № 3-1 - од

Политика информационной безопасности ГБСУСОССЗН «Ливенский дом социального обслуживания»

1. Общие положения и цели

1.1. Политика информационной безопасности государственного бюджетного стационарного учреждения социального обслуживания системы социальной защиты населения «Ливенский дом социального обслуживания»(далее - Политика) разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности.

1.2. Политика устанавливает цели, задачи и подходы в области информационной безопасности, которыми **ГБСУСОССЗН «Ливенский дом социального обслуживания»** (далее - учреждение) руководствуется в своей деятельности.

1.3. Политика направлена на достижение следующих целей:

- обеспечение непрерывности исполнения учреждением своих функций;
- минимизация возможных потерь и ущерба от нарушений в области информационной безопасности.

2. Управление информационной безопасностью

2.1. Для достижения указанных в п. 1.3. целей Политики в учреждении внедряется система управления информационной безопасностью (далее - СУИБ), которая соответствует законодательству Российской Федерации нормам права в части обеспечения информационной безопасности. СУИБ учреждения документирована в настоящей Политике, в правилах, положениях, рабочих инструкциях, которые являются обязательными для всех работников учреждения в области действия системы. Документированные требования СУИБ, кроме документов ограниченного использования, доводятся до сведения работников УСЗН.

2.2. Все информационные объекты учреждения, включая аппаратное обеспечение, программное обеспечение, информационные ресурсы подлежат учету в соответствии с их важностью и степенью доступа.

2.3. По результатам оценки рисков информационной безопасности выбираются и применяются средства управления для защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения информационной безопасности.

2.4. Для обеспечения физической защиты информационных объектов учреждение в границах области действия СУИБ (здание учреждения,

расположенное по адресу: Белгородская область. Красногвардейский район с. Ливенка, ул. Крупская д. 55.) устанавливаются зоны безопасности и принимаются меры для предотвращения несанкционированного доступа.

2.5. Учреждение стремится выявлять, учитывать и реагировать на инциденты в сфере информационной безопасности в соответствии с установленными процедурами.

2.6. В учреждении устанавливаются процедуры обеспечения непрерывности процессов от эффектов существенных сбоев информационных систем или чрезвычайных ситуаций, контроля работоспособности СУИБ.

2.7. Работники учреждения получают доступ к той информации, которая требуется им для исполнения своих должностных обязанностей.

2.8. Учреждение проводит информирование, обучение и повышение квалификации работников в сфере информационной безопасности в специализированных организациях.

3. Описание объекта защиты

3.1. Основными объектами защиты системы информационной безопасности в учреждении являются:

- информационные ресурсы, содержащие конфиденциальную информацию, включая персональные данные физических лиц, а также открыто распространяемая информация, необходимая для работы учреждения, независимо от формы и вида ее представления;
- персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы учреждения, независимо от формы и вида ее представления;
- сотрудники учреждения, являющиеся пользователями информационных систем учреждения;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

3.2. Руководство учреждения обеспечивает регулярный контроль за соблюдением настоящей политики в соответствии с установленными стандартами и процедурами контроля, определенных в рамках комплекта нормативных документов в области информационной безопасности.

3.3. Случаи несоблюдения настоящей Политики подлежат подробному расследованию и должны разрешаться в соответствии с действующим законодательством могут привести к лишению доступа к информационным системам, а также принятию дисциплинарных мер взыскания к виновным.

3.4. Любые преднамеренные действия, предпринимаемые с целью нарушить, блокировать, предоставить данные третьим лицам или иным способом обойти установленные средства контроля в области информационной безопасности, а также блокировать или противодействовать работе технических средств по регистрации или направлению сообщений о нарушениях в системе защиты, будут рассматриваться как потеря доверия и могут привести к принятию дисциплинарных мер.

3.5. ГБСУСОССЗН «Ливенский дом социального обслуживания», в лице руководителя или уполномоченного должностного лица, оставляет за собой право на просмотр любой информации, которая хранится, передается или

обрабатывается в ее компьютерных или телекоммуникационных системах и на соответствующих носителях данных, контролировать использование вычислительных ресурсов с точки зрения служебной необходимости, а также отказывать в предоставлении доступа или аннулировать доступ или принимать дисциплинарные меры взыскания к любому сотруднику с целью обеспечения соблюдения настоящей Политики.

4. Ответственность.

4.1. Руководство учреждения осуществляет общее управление информационной безопасностью учреждения и обеспечивает условия, необходимые условия для:

- реализации мероприятий по оценке рисков информационной безопасности и защиты информации;
- поддержания, мониторинга, анализа и непрерывного улучшения системы управления информационной безопасностью;
- обучения работников учреждения в сфере информационной безопасности в аккредитованных организациях.

4.2. Работники учреждения несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности.

4.3. В должностных инструкциях работников устанавливается ответственность за сохранность служебной документации и конфиденциальность информации, соблюдение правил обработки персональных данных, ставших известных в силу выполнения своих обязанностей.

5. Заключительные положения

Политика информационной безопасности учреждения является общедоступным документом, который должен предоставляться всем заинтересованным лицам и размещается на официальном сайте ГБСУСОССЗН «Ливенский дом социального обслуживания».