Российская Федерация
Муниципальное казенное учреждение
«Централизованная бухгалтерия
города Усолье-Сибирское»
(МКУ «ЦБ г. Усолье-Сибирское»)
ПРИКАЗ
19.12.2017г. № 330
г. Усолье-Сибирское

« Об утверждении Политики
информационной безопасности
в МКУ «ЦБ г. Усолье-Сибирское»

В целях исполнения законодательства Российской Федерации в области обеспечения информационной безопасности

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности в МКУ «ЦБ г. Усолье-Сибирское» (Приложение №1).
2. Заместителю директора Левиной О.А. организовать размещение данного приказа на странице официального сайта МКУ «ЦБ г. Усолье-Сибирское».
3. Инспектору по кадрам Спешиловой Т.Н. организовать ознакомление сотрудников МКУ «ЦБ г. Усолье-Сибирское», в том числе вновь поступающих на работу с настоящим приказом.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МКУ «ЦБ г. Усолье-Сибирское» Л.Ф.Шевнина

Приложение № 1
к приказу МКУ «ЦБ
г.Усолье-Сибирское»
от 19.12.2017г. № 330

Политика
информационной безопасности МКУ «ЦБ г. Усолье-Сибирское»

1. Общие положения и цели

1.1. Муниципальное казенное учреждение города Усолье-Сибирское» (далее – Учреждение), действующее на основании Устава, утвержденного постановлением администрации города Усолье-Сибирское от 12.11.2015г. № 2046.
1.2. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности.
1.3. Политика информационной безопасности (далее Политика) Учреждения устанавливает цели, задачи и подходы в области информационной безопасности, которыми Учреждение руководствуется в своей деятельности.
1.4. 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.1.4. Политики целей в Учреждении внедряется система управления информационной безопасностью (далее – СУИБ), которая соответствует законодательству Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов города Усолье-Сибирское.
2.2. 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 Учреждения.
2.3. Все информационные объекты Учреждения, включая программное обеспечение, информационные ресурсы на бумажных и электронных носителях подлежат учету и категорированию в соответствии с их важностью и степенью доступа.
2.4. 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.
2.5. Для обеспечения физической защиты информационных объектов Учреждения в границах области действия СУИБ (здание Учреждения, расположенное по адресу: г.Усолье-Сибирское, пр-кт Комсомольский,33) устанавливаются зоны безопасности и принимаются меры для предотвращения неавторизованного доступа.
2.6. Учреждение стремится выявлять, учитывать и реагировать на инциденты в сфере информационной безопасности в соответствии с установленными процедурами.
2.7. В Учреждении устанавливаются процедуры обеспечения непрерывности процессов от эффектов существенных сбоев информационных систем или чрезвычайных ситуаций, контроля работоспособности СУИБ.
2.8. Работники Учреждения получают доступ к той информации, которая требуется им для исполнения своих должностных обязанностей.
2.9. Учреждение проводит информирование, обучение и повышение квалификации работников в сфере информационной безопасности.

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;

– работники Учреждения, являющиеся пользователями информационных систем;

– 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.

4. Обеспечение соблюдения политики информационной безопасности и принятие мер в случае ее нарушения.

4.1. 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.

4.2. В целях проверки соблюдения информационной безопасности в Учреждении действует постоянно-действующая техническая комиссия (далее ПДТК), которая создаётся приказом руководителя.

4.3. Случаи несоблюдения настоящей Политики подлежат подробному расследованию и должны разрешаться в соответствии с действующим законодательством, НПА Учреждения, Правилами трудового распорядка и могут привести к лишению доступа к информационным системам, а также принятию дисциплинарных мер взыскания к виновным вплоть до увольнения.

4.4. Любые преднамеренные действия, предпринимаемые с целью нарушить, блокировать 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.

4.5. Учреждение 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.

5. Ответственность

5.1. Руководство Учреждения осуществляет общее управление информационной безопасностью Учреждения и обеспечивает необходимые условия для:

– реализации мероприятий по оценке рисков информационной безопасности и защиты информации;

– поддержания, мониторинга, анализа и непрерывного улучшения системы управления информационной безопасностью;

– регулярного обучения работников в сфере информационной безопасности.

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

5.3. 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.

6. Заключительные положения

6.1. Настоящая Политика, объявляется, распространяется, внедряется и поддерживается на всех уровнях Учреждения.

6.2. Политика информационной безопасности является общедоступным документом, который должен предоставляться всем заинтересованным лицам и размещается на странице официального сайта Учреждения.