Российская Федерация
Муниципальное казенное учреждение
«Централизованная бухгалтерия
города Усолье-Сибирское»
(МКУ «ЦБ г. Усолье-Сибирское»)

ПРИКАЗ

19.12.2017г. № 341

г. Усолье-Сибирское

« Об утверждении Парольной
политики МКУ «ЦБ г. Усолье-Сибирское»

В целях исполнения законодательства Российской Федерации в области обеспечения информационной безопасности

ПРИКАЗЫВАЮ:

1. Утвердить Парольную политику 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. № 341

Парольная политика
МКУ «ЦБ г. Усолье-Сибирское»

1. Общие положения

1.1. Парольная политика (далее – Политика) МКУ «Централизованная бухгалтерия города Усолье-Сибирское» (далее - Учреждение) разработана в соответствии с Концепцией безопасности информации Учреждения, и определяет требования к организации защиты информационно-вычислительной сети (далее – ИВС) от вредоносных программ, с целью предотвращения потери (искажения, перехвата) информации, заражения программного обеспечения, перегрузки и повреждения оборудования ИВС.

1.2. Политика является руководящим документом, единым для всего Учреждения и обязательным для выполнения всеми работниками Учреждения.

2. Обозначения и сокращения

АС – автоматизированная система
АРМ – автоматизированное рабочее место
ПО – программное обеспечение

3. Доступ к ПО

3.1. Доступ к используемому пользователями и администраторами в рамках должностных обязанностей и подразумевающему наличие идентификации и аутентификации пользователя и разграничение полномочий, без использования пароля запрещено. Пароли доступа к различному прикладному ПО, используемому пользователями и администраторами в рамках должностных обязанностей должны отличаться от паролей доступа к АРМ или элементам сетевой инфраструктуры и не должны совпадать для различного ПО.

Администраторам запрещено отклоняться от настоящей политики во имя удобства пользования.

3.2. Порядок создания пароля

Создание пароля должно предусматривать создание первичного пароля администратором, с последующей его сменой пользователем при первом запуске ПО. В случае если данная возможность не поддерживается ПО, пользователь обязан самостоятельно создать пароль пользователя при первом запуске ПО.

Пароли не должны передаваться в электронных сообщениях или любых иных формах электронного обмена.

3.3.Регулярность смены пароля

Системные пароли (например, пароль учетной записи Root, администратор, а также пароли обеспечивающие возможность полного управления) должны меняться регулярно, но не реже одного раза в три месяца. Пароли пользователей (например, пароли учетной записи, удаленного доступа к базам данным) должны меняться регулярно, но не реже одного раза в 3 месяца, если иное не определено НПА РФ и организационно- распорядительными документами Учреждения.

В случае компрометации пароля необходимо его немедленное изменение, а также оповещение о данном факте администратора информационной безопасности.

Внеплановая смена паролей пользователя производится в случае прекращения или изменения его полномочий (переход на другую работу внутри Учреждения и т.п.) немедленно после окончания последнего сеанса работы данного пользователя с АС.

Полная внеплановая смена всех системных паролей и паролей пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) любого из лиц, выполнявших должностные обязанности администратора и имевших доступ к паролям.

3.4. Восстановление пароля

Восстановление забытых паролей пользователей осуществляется администратором, путем сброса забытого пароля и установления первичного пароля, в случае если установка первичного пароля не поддерживается ПО, администратор осуществляет сброс забытого пароля, а пользователь обязан самостоятельно создать пароль пользователя при первом запуске ПО. Основанием для смены пароля может являться только заявка в письменной форме.

3.5. Хранение пароля и передача его третьим лицам

Пользователи не должны сообщать свои пароли третьим лицам, включая руководителей и лиц, осуществляющих сопровождение ПО. Администраторы АС не должны просить пользователей сообщить им их пароли.

Хранение пользователями любых паролей в электронном или физическом виде на любом, в том числе личном, носителе информации (в виде отдельных файлов, записей в ежедневниках, а также с применением функций ПО и т.п.), разрешено при условии исключения возможности получения доступа к паролям третьих лиц.

Хранение паролей администраторами (в том числе администратором информационной безопасности), допускается только при применении средств криптографической защиты, при этом хранение не зашифрованных системных паролей в электронном виде – запрещено.

Использование администраторами АС функций ПО, позволяющих исключить ввод пароля при повторных запусках, возможно в исключительных случаях (например, в системе резервного копирования, системе антивирусной защиты).

Допускается хранение пароля на индивидуальном носителе (смарт-карта, электронный идентификатор touch memory и т.д.). В таком случае пользователь несет персональную ответственность за сохранность данного индивидуального носителя, а также обязуется вернуть его по запросу структурного подразделения Учреждения, выдавшего его, или при прекращении полномочий.