Рассмотрено
на заседании Педагогического
совета Протокол № 2
от 16.10.2020 г.

«Утверждаю»
заведующий МБДОУ д/с № 22
п. Стодолище
_____ С.В. Мартынова
Приказ № 138 «А» от 27.10.2020 г.

Положение о парольной защите при обработке персональных данных и иной конфиденциальной информации в муниципальном бюджетного дошкольном образовательном учреждении детском саду № 22 п. Стодолище.

2020 г.

1. Общие положения

Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах (ИС) организации, а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями в муниципальном бюджетном дошкольном образовательном учреждении детском саду № 22 п. Стодолище (далее – ДОУ). Парольная защита требует соблюдения ряда правил, изложенных в настоящем Положении.

Цель: Положение определяет требования ДОУ к парольной защите информационных систем. Область действия Положения распространяется на всех пользователей и информационные системы (Далее – ИС) ДОУ, использующих парольную защиту.

2. Термины и определение ИС

В данном случае любая информационная система, для работы которой необходима аутентификация пользователя.

Пароль – секретный набор символов, используемый для аутентификации пользователя.

Пользователи – администраторы ИС и работники ДОУ, которым предоставлен доступ к ИС ДОУ, а также доступ к ресурсам сети Интернет.

Учётная запись – идентификатор пользователя, используемый для доступа к ИС.

3. Положения

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учётом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем реестрах, цифры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль Пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т д.) использование имён и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей сообщать руководителю их новые значения.

Внеплановая смена личного пароля или удаление учётной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т. п.) должна производиться сотрудниками, отвечающими за работу ИС немедленно после окончания последнего сеанса работы данного Пользователя с системой. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т. д.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС. Хранение Пользователем своих паролей на бумажном носителе допускается только в сейфе у руководителя в опечатанном конверте.

Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на заместителя заведующего.

4. Роли и ответственность

Пользователи:

Исполняют требования Положения и несут ответственность за её нарушение. Информируют администратора парольной защиты обо всех ставших им известных случаях нарушения настоящего Положения.

Администратор парольной защиты:

Принимает обращения пользователей по вопросам парольной защиты (например, блокировка четных записей, нарушение положения и др.). Организует консультации пользователей по вопросам использования парольной защиты. Контролирует действия Пользователей по вопросам использования парольной защиты. Контролирует действия Пользователей при работе с паролями, соблюдением порядка их смены,

хранения и использования. Отвечает за безопасное хранение паролей встроенных административных учётных записей.