УТВЕРЖДАЮ
Заведующий МБДОУ № 164
_____ Н.Г. Быкова
Приказ № 02/1-ОД
от «09» января 2018г.

# ИНСТРУКЦИЯ
# ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (ИСПДн) в муниципальном бюджетном дошкольном образовательном учреждении детском саду комбинированного вида № 164 города Ставрополя (далее Учреждение), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с идентификаторами и с личными паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей и контроль за действиями пользователей при работе с паролями возлагается на администратора безопасности информации.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующий требований:

- длина пароля должна быть не менее 6(шести) буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов(имена, фамилии, наименования АС и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 (шести) 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.

3.При наличии в случае возникновения нештатных ситуаций, форсмажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых пользователей в их отсутствие, такие пользователи обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение администратору безопасности информации или руководителю своего подразделения.

3. При наличии в случае возникновения нештатных ситуаций, форсмажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых пользователей в их отсутствие, такие пользователи обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение администратору безопасности информации или руководителю своего подразделения. Опечатанные конверты с паролями пользователей должны храниться в сейфе. Для опечатывания конвертов должны применяться личные печати владельцев паролей (при их наличии у пользователей).

4. В случае утечки информации о зарегистрированном пользователе необходимо НЕМЕДЛЕННО УДАЛИТЬ данные об этом пользователе и ЗАРЕГИСТРИРОВАТЬ ЗАНОВО его с новым идентификатором.

5. Пользователи, зарегистрированные для работы на информационной системе должны быть ознакомлены и предупреждены об ответственности за использование, хранение и потерю присвоенных идентификатора и пароля.

6. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

7. Внеплановая смена личного пароля или удаление учетной записи пользователя, в случае прекращения его полномочий (увольнение, переход на другую работу, в другое подразделение организации и т.п.) должно немедленно производиться стирание администратором безопасности информации о пользователе после окончания последнего сеанса работы данного пользователя в информационной системе.

8. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора безопасности информации.

9. В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры в соответствии с п.7 или п.8 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

10. Хранение пользователем зарегистрированных идентификаторов и значений своих паролей на бумажном носителе допускается только в сейфе у администратора безопасности информации.

11. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности информации.