Утверждено приказом
Заведующего МАДОУ ЦРР-детский сад№33
«Золушка» города Ишимбая
Ишимбайский район РБ
_____ Горяйнова А.Н.
Приказ № 07 от 14.01.2021г.

Инструкция

по организации парольной защиты

в Муниципальном автономном дошкольном образовательном учреждении центр развития ребёнка детский сад № 33 «Золушка» города Ишимбая муниципального района Ишимбайский район Республики Башкортостан

1.Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей на автоматизированных рабочих местах (АРМ) сотрудников Муниципального автономного дошкольного образовательного учреждения центр развития ребёнка - детский сад№ 33 «Золушка» города Ишимбая муниципального района Ишимбайский район Республика Башкортостан (далее по тексту – организация)
2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на компьютерах пользователей возлагается на специалиста организации.
3.Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на серверах возлагается на специалиста.

4. Личный пароль должен генерировать и распределять централизованно либо выбираться пользователем автоматической системы самостоятельно с учетом следующих требований:

-длина пароля должна быть не менее 6 символов;

- пароль не должен включать в себя легко вычисляемые сочетание символов, а также общепринятые сокращения (ЭВМ, ЛВС, wster 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,

5. Владелец пароля должен быть ознакомлен под роспись с перечисленными выше требованиями и предупрежден об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
6. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей сотрудника (исполнителя) в его отсутствие, сотрудник обязан сразу же сменить свой пароль на новый.
7. Плановая смена паролей пользователя должна проводиться регулярно, не реже одного раза в 6 месяцев.
8. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.
9. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.
10. Пароли пользователей (вместе с именами соответствующих учетных записей) должны храниться в запечатанном конверте в сейфе руководителя организации.
11. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.
12. Пользователю следует помнить, что при смене пароля на компьютере пользователя доступ к сетевым ресурсам под новым паролем без соответствующей смены пароля на сервере невозможен.