ПРИНЯТО
на заседании педагогического совета
КОГОБУ ВСШ г. Омутнинска
Протокол от 31.05.2016 № 7

УТВЕРЖДАЮ
Директор КОГОБУ ВСШ г. Омутнинска
_____ Т.А. Сюзева
Приказ от 31.05.2016 № 28

ПОЛИТИКА
назначения и смены паролей
Кировского областного государственного общеобразовательного бюджетного учреждения «Вечерняя средняя школа г. Омутнинска»

Настоящая политика определяет порядок обеспечения надежных средств идентификации и проверки подлинности пользователей и администраторов, хранящих и обрабатывающих конфиденциальную информацию на автоматизированных рабочих местах (далее – АРМ).

1. Ответственным за обеспечение выполнения настоящей политики является Администратор безопасности конфиденциальной информации.
2. Установку первичного пароля производит Администратор безопасности конфиденциальной информации. Ответственность за сохранность первичного пароля лежит на администраторе, установившем данный пароль.
3. При создании первичного пароля Администратор безопасности конфиденциальной информации обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.
4. Первичный пароль не используется при сбросе забытого пароля на учетную запись, необходима установка нового пароля.
5. Установку нового пароля производит пользователь при первом в систему с новой учетной записью.
6. Личные пароли должны выбираться с учетом требований:

6.1. Длина пароля не менее шести символов;

6.2. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, числа, сочетания цифр и т.п.), а также общепринятые сокращения (ЭВМ, USER и т.п.);

6.3. Пароль не должен содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков;

6.4. Содержать знаки трех или четырех перечисленных категорий: латинские заглавные буквы, латинские строчные буквы, цифры, отличающиеся от букв и цифр знаки;

6.5. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-ех позициях.

7. Пользователь несет персональную ответственность за сохранение в тайне нового пароля.
8. Пользователям запрещается:
   8.1. Записывать пароль и хранить его в легкодоступных местах, в том числе на мониторе, рабочем столе или ящиках стола;
   8.2. Сообщать пароль другим лицам;
   8.3. Пересылать открытым текстом в электронных сообщениях;
   8.4. Подбирать пароли других пользователей.
9. Пользователи обязаны сообщать Администратору безопасности конфиденциальной информации о всех случаях попыток противоправных действий пользователей в отношении других пользователей.
10. Полная плановая смена паролей должна проводиться регулярно, не реже одного раза в шесть месяцев для пользователей и не реже одного раза в двенадцать месяцев для администраторов и других технологических учетных записей.
11. Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий в организации (увольнение, перевод на другую должность) должна производиться Администратором безопасности конфиденциальной информации немедленно после окончания последнего сеанса работы данного пользователя с системой.
12. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий Администратора безопасности конфиденциальной информации.
13. В случае компроментации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.11 или п. 12 настоящей Политики в зависимости от полномочий владельца скомпроментированного пароля.
14. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в сейфе, либо в сейфе Администратора безопасности конфиденциальной информации.

15. При возникновении нештатных ситуаций, форс-мажорных обстоятельств, которые влекут необходимость доступа к информации пользователя, отсутствующего на рабочем месте, по решению Руководителя ОО может быть инициирован сброс пароля данного пользователя Администраторм безопасности конфиденциальной информации и осуществлен доступ к необходимой информации. По факту такого доступа составляется акт, описывающий условия осуществления доступа, который подписывается Руководителем ОО, Администратором безопасности конфиденциальной информации и сотрудником, запросившем доступ.
16. Пользователи должны быть ознакомлены под подпись с настоящей инструкцией. Повседневный контроль за действиями исполнителей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора безопасности конфиденциальной информации.