Приложение №4
к Положению «Об обработке и защите персональных данных в Государственном бюджетном профессиональном образовательном учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»»

Инструкция по организации парольной защиты

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей), а также контроль за действиями пользователей и обслуживающего персонала при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использование и прекращение действия паролей во всех информационных системах и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на специалиста по защите информации Колледжа.

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

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать латинские буквы и цифры;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения, 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 4 позициях;

– личный пароль пользователь не имеет права сообщать никому.

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

3. После использования имен и паролей некоторых работников (исполнителей) в их отсутствие, при наличии технологической необходимости в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п., работники обязаны сразу же сменить свой пароль.

4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в год.

5. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться специалистом по защите информации немедленно после окончания последнего сеанса работы данного пользователя на ПК.

6. В случае компрометации личного пароля пользователя должны быть немедленно приняты меры в соответствии с п. 5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Хранение работником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем сейфе.

Приложение №5
к Положению «Об обработке и защите персональных данных в Государственном бюджетном профессиональном образовательном учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»»

Инструкция по организации антивирусной защиты

Общие положения

1. Настоящая инструкция определяет правила, которыми должны руководствоваться работники при организации антивирусной защиты.
2. Целью защиты является предотвращение ущерба от действий, производимых вирусами и другими вредоносными программами.

Область применения

Положения настоящей инструкции распространяются на все работы, связанные с обеспечением антивирусной защиты в Колледже, а также на всех работников, которым предоставлен доступ к информационным ресурсам Колледжа.

Правила использования средств антивирусной защиты

1. К использованию допускаются только лицензионные антивирусные средства.
2. Установка и настройка параметров средств антивирусного контроля на рабочих станциях и серверах Колледжа осуществляется специалистом по защите информации.
3. Обновление антивирусных средств должно происходить в автоматическом режиме. Допускается работа антивируса с обновлениями не старше 72 часов.
4. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться еженедельно.
5. На каждой рабочей станции и сервере в резидентном режиме должен быть запущен антивирусный монитор.
6. Обязательному антивирусному контролю подлежит любая информация, получаемая по телекоммуникационным каналам связи и на съемных носителях.
7. Устанавливаемое программное обеспечение должно быть предварительно проверено на наличие вирусов.
8. Каждый пользователь должен быть осведомлен об опасности заражения вирусами и обучен работе с антивирусным программным обеспечением.

Ответственность

Ответственность за организацию антивирусного контроля в подразделении возлагается на специалиста по защите информации. Ответственность за проведение мероприятий антивирусного контроля в подразделении возлагается на ответственного за обеспечение безопасности информации. За нарушение положений данной инструкции работники Колледжа могут быть отстранены от доступа к информационным ресурсам Колледжа и несут ответственность в соответствии с законодательством Российской Федерации.

Приложение №6
к Положению «Об обработке и защите персональных данных в Государственном бюджетном профессиональном образовательном учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»»

Инструкция
«О порядке обеспечения сохранности документов, дел и изданий, содержащих сведения конфиденциального характера»

1. Все имеющиеся документы, дела и издания, содержащие конфиденциальную информацию, должны храниться в служебных помещениях в надежно запираемых шкафах или сейфах. Помещения должны отвечать требованиям режима, обеспечивающего физическую сохранность находящейся в них документации. При необходимости шкафы, сейфы и служебные помещения могут опечатываться личными металлическими номерными печатями работников. Дубликаты ключей от шкафов и сейфов, в которых хранятся конфиденциальные документы, сдаются в опечатанных конвертах уполномоченному лицу.

2. Конфиденциальные документы хранятся (в шкафах или сейфах) отдельно от неконфиденциальных документов. При совместном хранении конфиденциальные документы группируются в папках (скоросшивателях), чтобы отделить их от неконфиденциальных документов.

3. Запрещается оставлять на рабочих местах без присмотра или в незапертых шкафах (сейфах) конфиденциальные документы в течение рабочего дня или по его окончании.

4. Доступ посторонних лиц в помещения, предназначенные для работы с конфиденциальной информацией, по возможности, ограничивается. Для работы с посетителями используются отдельные места для переговоров.

При нахождении в помещении, где проводится работа с конфиденциальными документами, посторонних лиц (в том числе сотрудников, не допущенных к данным сведениям), документы должны убираться в шкаф или сейф, чтобы исключить случайное ознакомление посторонних с конфиденциальными документами.

5. С конфиденциальными документами разрешается работать только в служебных помещениях. Для работы вне служебных помещений необходимо разрешение руководителя структурного подразделения.

6. Конфиденциальные документы могут передаваться для работы и временного хранения другим работникам, допущенным к этим документам, только под расписку. Передача подобных документов, дел, изданий в другие подразделения на постоянное хранение осуществляется через директора Колледжа.

7. Уничтожение конфиденциальных документов проводится в порядке, установленном локальным нормативным актом Колледжа.

Приложение №7
к Положению «Об обработке и защите персональных данных в
Государственном бюджетном профессиональном образовательном
учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»»

Журнал обращений по ознакомлению с персональными данными
(форма)

№ п/п	Фамилия, имя, отчество	Адрес субъекта ПД	Дата обращения. Содержание обращения	Дата ответа. Принятое решение

Приложение №8
к Положению «Об обработке и защите персональных данных в Государственном бюджетном профессиональном образовательном учреждении «Пензенский музыкальный колледж им. А.А. Архангельского»»

Журнал учета съемных носителей персональных данных (форма)

№ п/п	Метка съемного носителя (учетный номер)	Фамилия, инициалы исполнителя	(Получил, вернул, передал)	Дата записи информации	Подпись исполнителя