РАССМОТРЕН
на заседании Совета Учреждения
ГБПОУ «СГХТ»
Протокол № 4
«21» декабря 2017 г.

УТВЕРЖДАЮ
Директор ГБПОУ «СГХТ»
_____ /А. В. Капыл/
«25» декабря 2017 г.

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

ПОЛОЖЕНИЕ

об отделе по информационным технологиям

СМК-ПО-01-08-61-2017

Версия 01

Введено впервые

РАЗРАБОТАНО:
представитель руководства по качеству _____ О.Н. Бобровских

СОГЛАСОВАНО:
Заведующий отделом по ИТ _____ Д.А. Костылев

Дата принятия «25» декабря 2017г.,
приказ по техникуму № 01-03-218 от 25.12.2017

Настоящий документ является внутренним документом ГБПОУ «СГХТ»

1. Общие положения

1.1. Отдел по информационным технологиям (далее – отдел по ИТ) является структурным подразделением государственного бюджетного профессионального образовательного учреждения «Соликамский горно-химический техникум» (далее - техникум). Он создается для развития информационного обеспечения управления, развития информационного обеспечения учебного процесса техникума, организации электронного документооборота, контроля работы серверного оборудования, технического обслуживания компьютеров и оргтехники техникума и т. п.

1.2. Отдел по ИТ создается и ликвидируется приказом директора техникума.

1.3. Отдел по ИТ возглавляет заведующий отделом по ИТ, назначаемый на должность приказом директора техникума

1.4. Отдел по ИТ подчиняется непосредственно заместителю директору техникума..

1.5. Сотрудники отдела по ИТ назначаются на должности и освобождаются от должностей приказом директора техникума по представлению заведующего отделом по ИТ.

1.6. В своей деятельности отдел руководствуется:

- действующим российским законодательством;
- Уставом техникума;
- Правилами внутреннего распорядка;
- приказами и распоряжениями директора техникума;
- настоящим положением.

2. Основные задачи и функции

2.1. Развитие информационного обеспечения управления.

2.2. Информационное обеспечение учебного процесса техникума.

2.3. Сопровождение работы электронного документооборота.

2.4. Техническое обслуживание компьютеров и оргтехники техникума.

2.5. Информационное сопровождение учебного процесса.

2.6. Технические работы по вводу и изменению информации в компьютере по заявкам.

2.7. Профилактические работы на сервере и рабочих станциях.

2.8. Установка программного обеспечения.

2.9. Оперативный ремонт и переустановка программного обеспечения.

2.10. Обеспечение готовности компьютеров на момент использования в учебном процессе.

2.11. Своевременное обеспечение расходными материалами по заявкам пользователей ПК.

2.12. Проведение единой технической политики, организация и координация работ по обеспечению безопасности персональных данных в соответствующей организации.

2.13.Проведение мероприятий по организации обеспечения безопасности персональных данных, включая классификацию информационных систем персональных данных.

2.14. Проведение мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в том числе

- мероприятия по закрытию технических каналов утечки персональных данных при их обработке;

- мероприятия по защите от несанкционированного доступа к персональным данным;

- мероприятия по выбору средств защиты персональных данных при их обработке.

2.15. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передачи их лицам, не имеющим права доступа к такой информации.

2.16. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

2.17. Недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование.

2.18. Обеспечение возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.19. Постоянный контроль за обеспечением уровня защищенности персональных данных.

2.20. Участие в подготовке объектов соответствующей организации к аттестации по выполнению требований обеспечения безопасности персональных данных.

2.21. Разработка организационных распорядительных документов по обеспечению безопасности персональных данных в соответствующей организации.

2.22. Организация в установленном порядке расследования причин и условий появления нарушений в безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.

2.23. Разработка предложений, участие в проводимых работах по совершенствованию системы безопасности персональных данных в соответствующей организации.

2.24. Проведение периодического контроля эффективности мер защиты персональных данных в соответствующей организации. Учет и анализ результатов контроля.

2.25. Организация повышения осведомленности руководства и сотрудников в соответствующей организации по вопросам обеспечения безопасности персональных данных, сотрудников подведомственных предприятий, учреждений и организаций.

2.26. Подготовка отчетов о состоянии работ по обеспечения безопасности персональных данных в соответствующей организации.

2.27. Планирование информационной инфраструктуры, структуры внутренней сети.

2.28. Организация и обеспечивает бесперебойного функционирования локальной вычислительной сети. Мониторинг использования локальной вычислительной сети.

2.29. Установка на серверы и рабочие станции сетевого программного обеспечения, конфигурирование систем и программного обеспечения на серверах.

2.30. Организация доступа к локальным и глобальным сетям, в том числе - сеть Интернет.

2.31. Регистрация пользователей, назначение идентификаторов (логинов) и паролей.

2.32. Установка и настройка сетевых сервисов. Поддержание их в рабочем состоянии.

2.33. Обучение и консультирование пользователей при работе в локальной вычислительной сети, сети Интернет, использовании электронной почты, ведению архивов.

2.34. Протоколирование системных и сетевых событий, событий доступа к ресурсам - для последующего анализа.

2.35. Защита от вирусов. Обновление антивирусных баз.

2.36. Установка ограничений для пользователей по: использованию рабочей станции или серверов; времени; степени использования ресурсов.

2.37. Составление заявки на ремонт неисправного, а также приобретение нового и модернизацию устаревшего аппаратного оборудования серверов и рабочих станции, а также сетевого оборудования.

2.38. Техническое обслуживание электронной техники путем регламентации проведения профилактических работ, обеспечивает ее работоспособное состояние, рациональное использование.

2.39. Контроль за соблюдением инструкций по эксплуатации, техническому уходу за компьютерным оборудованием.

2.40. Работа и администрирование официального сайта Техникума.

3. Структура

3.1. Отдел по ИТ состоит из заведующего отделом по ИТ, сетевого администратора.

4. Права и ответственность

Отдел по ИТ имеет право:

4.1. Самостоятельно определять содержание и конкретные формы своей деятельности с целями и задачами, указанными в положении об отделе информационных технологий.

4.2. Представлять на рассмотрение и утверждение директору техникума проекты документов: правила по технике безопасности при выполнении работ, положения, должностные инструкции и др.

4.3. Вносить предложения по штатному расписанию, должностным окладам, надбавкам и доплатам сотрудникам в соответствии с действующими нормативами, в пределах фонда заработной платы.

4.4. Представлять техникум в различных учреждениях и организациях в пределах своей компетенции, принимать участие в работе конференций, совещаний и семинаров.

4.5. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных данных.

4.6. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.

4.7. Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.

4.8. Контролировать деятельность структурных подразделений соответствующей организации в части выполнения ими требований по обеспечению безопасности персональных данных.

4.9. Вносить предложения руководителю организации о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.

4.10. Привлекать в установленном порядке необходимых специалистов из числа сотрудников соответствующей организации для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

4.11. Отдел информационных технологий несет ответственность за сохранность переданных ему материальных ценностей. Работники виновные, в причинении ущерба имуществу техникума, переданному отделу, несут ответственность в порядке, предусмотренном действующим законодательством.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номера листов			Основание для внесения изменений	Подпись	Расшифровка подписи	Дата	Дата введения изменения
	заменен-ных	новых	аннулиро-ванных					