Российская Федерация
Муниципальное казенное учреждение
«Централизованная бухгалтерия
города Усолье-Сибирское»
(МКУ «ЦБ г. Усолье-Сибирское»)

ПРИКАЗ

19.12.2017г. № 336

г. Усолье-Сибирское

« Об утверждении Правил
обеспечения безопасности при
работе пользователей в
корпоративной сети
в МКУ «ЦБ г. Усолье-Сибирское»

В целях исполнения законодательства Российской Федерации в области обеспечения информационной безопасности

ПРИКАЗЫВАЮ:

1. Утвердить Правила обеспечения безопасности при работе пользователей в корпоративной сети МКУ «ЦБ г. Усолье-Сибирское» (Приложение №1).
2. Заместителю директора Левиной О.А. организовать размещение данного приказа на странице официального сайта МКУ «ЦБ г. Усолье-Сибирское».
3. Инспектору по кадрам Спешиловой Т.Н. организовать ознакомление сотрудников МКУ «ЦБ г. Усолье-Сибирское», в том числе вновь поступающих на работу с настоящим приказом.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МКУ «ЦБ г. Усолье-Сибирское» Л.Ф.Шевнина

Приложение № 1
к приказу МКУ «ЦБ
г.Усолье-Сибирское»
от 19.12.2017г. № 336

Правила
обеспечения безопасности при работе пользователей в корпоративной сети МКУ «ЦБ г. Усолье-Сибирское»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящие Правила регламентирует работу пользователей корпоративной компьютерной сети (далее – ККС) муниципального казенного учреждения «Централизованная бухгалтерия города Усолье-Сибирское» (далее - Учреждение) на рабочих местах.

1.2 ККС Учреждения состоит из логических сегментов сети (далее ЛСС) разделённых по функциональному признаку и представляет собой систему объектов вычислительной техники, содержащих информационные ресурсы, используемые в целях обеспечения видов деятельности Учреждения.

1.3 Пользователями ККС являются работники Учреждения, а также привлеченные по договорам специалисты.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

Пользователь обязан:

2.1) при обнаружении попыток несанкционированного доступа, подозрении на наличие вируса, других проблем в использовании ККС немедленно сообщать об этом администраторам ЛСС и (или) администратору информационной безопасности;

2.2) согласовывать с Администрацией ККС Учреждения проведение работ, предполагающих интенсивную загрузку ККС или большое количество сетевых соединений;

2.3) обеспечивать доступ к сетевому оборудованию и компьютеру пользователя Администраторам ЛСС Учреждения;

2.4) сохранять после окончания обработки конфиденциальных данных, не содержащих персональные данные, файлы, необходимые в дальнейшем, только в специально предназначенной для этого папке на отведённом сервере, а также по окончании рабочего дня произвести стирание остаточной информации с жесткого диска объекта вычислительной техники;

хранить файлы, предназначенные для совместной работы сотрудниками подразделения в специально отведенной папке «Общая папка бухгалтерии.

2.5) выполнять требования «Инструкции об организации парольной защиты на объектах вычислительной техники», касающиеся порядка создания, изменения, сохранения в тайне личной учетной записи;

2.6) выполнять требования антивирусной защиты, установленные «Инструкцией по организации антивирусной защиты на объектах вычислительной техники».

3. ЗАПРЕТЫ

Пользователю запрещается:

3.1) самовольно подключать компьютер к ККС Учреждения;

3.2) использовать каналоемкие ресурсы (real video, real audio, и др.) и аппаратные средства, которые могут привести к перегрузке сети, без согласования с Администрацией ККС Учреждения;

при сильной перегрузке канала в связи с использованием каналоемких ресурсов текущий сеанс пользователя, вызвавшего перегрузку, будет остановлен;

3.3) устанавливать на компьютере дополнительные сетевые службы (FTP, SSH, Telnet, DNS, DHCP, WWW, POP3, IMAP4, Proxy и др.), не предусмотренные по умолчанию операционной системой, или программное обеспечение, предоставляющее данные службы без согласования с Администрацией ККС Учреждения;

3.4) использовать иные способы доступа к сети Интернет, за исключением разрешенных Администрацией ККС Учреждения;

3.5) самовольно изменять сетевые настройки компьютера, в том числе:

- MAC-адрес;
- IP-адрес;
- сетевые клиенты, службы и протоколы;
- установка сетевых настроек компьютера может проводиться только Администраторами ЛВС и ККС Университета.

3.6) осуществлять сканирование сети и подбор паролей к сетевым ресурсам других пользователей;

3.7) осуществлять несанкционированный доступ к компьютерам, серверам или другим устройствам сети;

3.8) разрабатывать или распространять любые виды компьютерных вирусов, "троянских коней" или "логических бомб";

3.9) сообщать собственные пароли другим лицам, работать в сети под чужой учетной записью, разрешать посторонним лицам пользоваться компьютером;

3.10) использовать несуществующие обратные адреса при отправке электронных писем;

3.11) осуществлять рассылку несанкционированной коммерческой почтовой корреспонденции (SPAM);

3.12) использовать ресурсы ККС Учреждения в личных целях для получения коммерческой выгоды;

3.13) распространять через сеть информацию, запрещенную законодательством РФ;

3.14) нарушать авторские права, повреждать, уничтожать или фальсифицировать не принадлежащие пользователю информационные ресурсы, представленные в ККС Учреждения;

3.15) распространять информацию, противоречащую нормам морали и нравственности, порочащую честь и достоинство граждан, а также рассылать обманные или угрожающие сообщения;

3.16) распространять информацию порнографического характера, а также призывающую к национальной дискриминации или насилию.

4. ПРАВА ПОЛЬЗОВАТЕЛЯ

Пользователь имеет право:

4.1) использовать в работе ресурсы ККС Учреждения в оговоренных настоящей Инструкцией пределах;

4.2) обращаться за консультациями по вопросам работы в ККС Учреждения к администраторам ЛСС;

4.3) обращаться по вопросам работоспособности внешних каналов связи в Администрацию ККС Учреждения;

4.4) вносить предложения по улучшению работы с ресурсами ККС Учреждения администраторам ЛСС.

5. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ

5.1. Нарушение настоящей Инструкции влечет за собой в зависимости от характера нарушения административную, дисциплинарную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ и (или) отстранение пользователя от работы в ККС Учреждения.

5.2. При обнаружении компьютера, с которого производятся запрещенные настоящей Инструкцией действия, Администрация ККС Учреждения, без дополнительного уведомления, производит отключение данного компьютера от ККС Учреждения и блокирует доступ к ресурсам для учетной записи пользователя, под которой осуществлен вход на данный компьютер. Подключение компьютера к сети и разблокировка учетной записи выполняется только после письменного распоряжения руководителя Учреждения.