БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ
ДЛЯ ДЕТЕЙ-СИРОТ И ДЕТЕЙ, ОСТАВШИХСЯ БЕЗ ПОПЕЧЕНИЯ РОДИТЕЛЕЙ,
ВОЛОГОДСКОЙ ОБЛАСТИ «ВЕЛИКОУСТЮГСКИЙ ЦЕНТР ПОМОЩИ ДЕТЯМ,
ОСТАВШИМСЯ БЕЗ ПОПЕЧЕНИЯ РОДИТЕЛЕЙ»

С УЧЕТОМ МНЕНИЯ
Совета учреждения
Протокол от 29.08.2017 №26

УТВЕРЖДАЮ
Директор Н.Н. Долгина
Приказ от 06.09.2017 № 93

# ИНСТРУКЦИЯ ОБ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

## 1. Общие положения

1.1. Настоящая Инструкция об организации парольной защиты персональных компьютеров, содержащих персональные данные, в бюджетном учреждении социального обслуживания для детей-сирот и детей, оставшихся без попечения родителей, Вологодской области «Великоустюгский центр помощи детям, оставшимся без попечения родителей» (далее – Учреждение) регламентирует организационно-техническое обеспечение процессов генерации, использования, смены и прекращения действия личных паролей пользователей персональных компьютеров, содержащих персональные данные.

1.2. Список персональных компьютеров, содержащих персональные данные, содержится в журнале учета применяемых носителей информации в Учреждении, содержащих персональные данные в электронном виде.

1.3. Организационное и техническое обеспечение процессов использования, смены и прекращения действия паролей пользователей возлагается на заместителя директора по административно – хозяйственной работе.

1.4. Эффективность парольной защиты, выполнение требований ее организации контролируется заместителем директора по административно – хозяйственной работе.

## 2. Правила формирования личного пароля

2.1. В целях обеспечения защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий каждому пользователю персонального компьютера Учреждения, содержащего персональные данные, должно быть присвоено уникальное имя (учетная запись) с паролем.

2.2. Личные пароли определяются заместителем директора по административно – хозяйственной работе с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и/или нижнем регистрах, цифры и/или специальные символы (%,S,@, &, *, #, и т.п.);

- запрещается при авторизации пользователя использовать только логин (имя пользователя) без пароля;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена и даты рождения своей личности и своих родственников, номера автомобилей, телефонов и т.д.), которые можно угадать, основываясь на информации о пользователе, а также стандартное расположение букв на клавиатуре (zyxwvuts, 123, 123321, qwerty и т.д.);
- запрещается выбирать пароли, которые уже использовались ранее;
- пользователь не имеет права разглашать свой личный пароль.

## 3. Ввод пароля

3.1. Ввод пароля осуществляется с учетом регистра (верхний-нижний) и с учетом текущей раскладки клавиатуры (EN-RU и др.).

3.2. Во время ввода паролей необходимо исключить возможность распознания его посторонними лицами или компрометации пароля посредством технических средств.

## 4. Правила эксплуатации, хранения, смены и блокирования пароля

4.1. Владельцам паролей запрещается:
- сообщать другим пользователям личный пароль;
- записывать пароли в электронной записной книжке, файле и других носителях информации, кроме бумажных носителей, при этом бумажные носители с записями паролей должны храниться в надежном и доступном только владельцу месте.

4.2. Пароли сотрудников с именами учетных записей и датой установки паролей должны храниться в сейфе в кабинете директора Учреждения.

4.3. В случае компрометации личного пароля, пользователь должен немедленно известить заместителя директора по административно – хозяйственной работе, которому необходимо произвести внеплановую смену пароля.

4.4. При возникновении производственной необходимости в срочном доступе к данным персонального компьютера временно отсутствующего пользователя разрешается заместителю директора по административно – хозяйственной работе.

4.5. Ответственность за неразглашение полученного пароля и действия, произведенные на персональном компьютере, возлагается на лицо, получившее пароль после такого случая.

4.6. В течение 24 часов после увольнения работника заместитель директора по административно – хозяйственной работе блокирует учетную запись.

4.7. Контроль за действиями пользователей при работе с паролями возлагается на заместителя директора по административно – хозяйственной работе.

## 5. Ответственность при организации парольной защиты

5.1. За разглашение парольной информации работник, допустивший нарушение, привлекается к дисциплинарной ответственности в соответствии с законодательством Российской Федерации.

5.2. Пользователь обязан проводить процедуру блокировки персонального компьютера при оставлении своего рабочего места.