



ПАРОЛИ ПОЛЬЗОВАТЕЛЕЙ  
ИДЕНТИФИКАЦИЯ, ИСПОЛЬЗОВАНИЕ И  
ПРОЦЕДУРЫ ПО ЕГО ЗАЩИТЕ  
О ПРИНЦИПАХ  
ПРАВИЛА

КВКК\_У7 ВЕРСИЯ 1.00

## 1. ВВЕДЕНИЕ, ЦЕЛИ И ОПРЕДЕЛЕНИЯ

1.1. Настоящий Регламент определяет применимые процедуры и предоставляет пользователям рекомендации по использованию и/или защите паролей пользователей, определенных/подлежащих определению в отношении всех типов информационных и коммуникационных систем, используемых в Компании.

## 2. Принципы создания надежного пароля

2.1. Компания рассчитывает, что пользователи обеспечат эффективную защиту паролей, создавая надежные пароли, соответствующие следующим критериям: 2.1.1. Пароль должен содержать не менее 8 символов. 2.1.2. Пароль должен содержать не менее трех из следующих элементов:

- (I) Цифровые символы (0-9)
- (II) Заглавные буквы (AZ)
- (III) Строчные буквы (несколько)
- (IV) Специальные символы (?, !, @, #, %, и т. д.)

2.1.3. Пароль не должен содержать ничего из следующего:

(I) Слово, взятое из словаря (любого языка), сленг или общее сокращение.

(II) Название человека или места.

(III) Легко угадываемая дата, например, день рождения супруга/партнера пользователя.

(IV) Информация, заведомо относящаяся к пользователю, такая как номерной знак транспортного средства пользователя, идентификационный номер гражданина Турецкой Республики и номер карты доступа.

(V) Имя пользователя учетной записи должно совпадать или быть похожим на (включая имена пользователей, написанные в обратном порядке или с ошибками).

(VI) Любые пароли, информация и т. д., приведенные в качестве примеров на корпоративном веб-сайте компании или в настоящем Положении.

2.1.4. Новый пароль не может совпадать ни с одним из шести последних **использованных** паролей.

## 3. ПРИНЦИПЫ ЗАЩИТЫ ПАРОЛЕЙ

3.1. Пользователям следует выбирать запоминающиеся пароли, избегать ввода паролей вручную и ни при каких обстоятельствах не оставлять пароли в местах, где к ним легко могут получить доступ другие лица.

3.2. Пользователи не должны разглашать свои пароли другим лицам. Компания никогда не будет запрашивать пароль пользователя. Единственный человек, которому нужен ваш пароль, — это сам пользователь. Если пользователь получает электронное письмо, сообщение и т. д., содержащее подобный запрос, это сообщение следует рассматривать как попытку электронного мошенничества, и об этом следует немедленно сообщить ИТ-менеджеру, не отвечая на его запросы.

3.3. Если пользователь обнаружит, что его пароль был случайно или иным образом разглашен, он должен немедленно изменить свой пароль и незамедлительно сообщить об этом ИТ-менеджеру.

3.4. Пользователи должны обеспечить, чтобы другие не видели их экраны во время ввода пароля для входа в систему, и не должны располагать экраны таким образом, чтобы кто-либо, включая коллег, мог видеть, как они вводят пароль. Экраны также должны быть размещены в офисе таким образом, чтобы их не было видно извне здания.

3.5. Пользователям не следует вводить свои пароли на веб-сайте, если они не уверены, что это официальная корпоративная информационная и коммуникационная система/веб-сайт Компании. Лучший способ убедиться в этом — добавить сайты в закладки.

Это предполагает указание собственных URL-адресов или доступ к ним с помощью введенных вами URL-адресов.

Избегайте использования ссылок, особенно тех, которые содержатся в электронных письмах, выдающих себя за подлинные.

#### 4. ИЗМЕНЕНИЕ ПАРОЛЕЙ

- 4.1. Пользователям необходимо регулярно менять свои пароли. Заместитель генерального директора может установить период смены пароля в диапазоне от 30 дней до одного года в зависимости от ролей и обязанностей владельцев учетных записей, уполномоченных компанией.
- 4.2. Вы можете изменить свой пароль, войдя в систему на компьютерах, зарегистрированных в реестре компании, и воспользовавшись следующей ссылкой:  
<http://www.kardelenboya.com.tr/>
- 4.3. Повторное использование старых паролей не допускается. Это хорошая практика, и вы можете применять ее и к системам за пределами компании.
- 4.4. Пользователи, чьи пароли не соответствуют положениям настоящего Регламента, будут немедленно обязаны сменить свои пароли.
- 4.5. С пользователями, которым необходимо изменить свои пароли, свяжется сотрудник компании по электронной почте, телефону или лично. После этого пользователи смогут изменить свои пароли в компании.  
Ему не следует никому об этом рассказывать, включая своих сотрудников.

#### 5. Пароли для использования во внешних системах

- 5.1. Рекомендуется применять описанные в настоящем Положении передовые методы использования при работе с системами, не принадлежащими Компании.
- 5.2. Избегайте использования существующих имени пользователя и пароля в рамках Компании для создания учетных записей на веб-сайтах или других интернет-ресурсах.

