USER PASSWORDS IDENTIFICATION, USE AND PROCEDURES REGARDING ITS PROTECTION ABOUT THE PRINCIPLES REGULATIONS

KVKK_Y7 VERSION 1.00

1. INTRODUCTION, OBJECTIVES AND DEFINITIONS

1.1. This Regulation defines the applicable procedures and provides recommendations to users regarding the use and/or protection of user passwords defined/to be defined in relation to all types of information and communication systems used within the Company.

2. PRINCIPLES FOR DEFINING A STRONG PASSWORD

2.1. The company anticipates that users will ensure effective password protection by defining strong passwords, adhering to the following criteria: 2.1.1. The password must be at least 8 characters long. 2.1.2. The password must contain at least three of the following elements:

(I) Numeric characters (0-9)
(II) Capital letters (AZ)
(III) Lowercase letters (few)
(IV) Special characters (?, !, @, #, %, etc.)

2.1.3. The password must not contain any of the following:

(I) A word taken from a dictionary (of any language), slang, or general abbreviation.

(II) The name of a person or place.
(III) An easily guessable date, such as the birthday of the user's spouse/partner.

(IV) Information known to be related to the user, such as the user's vehicle license plate, Turkish Republic Identity Number, and access card number.
(V) The account username must be the same as or similar to (including reversed or misspelled usernames)
(VI) Any passwords, information, etc. given as examples on the company's corporate website or in this Regulation.

2.1.4. The new password cannot be the same as any of the last six passwords used.

3. PRINCIPLES TO FOLLOW FOR PASSWORD PROTECTION

3.1. Users should choose a memorable password, avoid typing passwords, and under no circumstances should they leave passwords in a place where others can easily access them.

3.2. Users should not disclose their passwords to others. The company will never ask for a user's password. The only person who needs to know your password is the user themselves. If a user receives any email, message, etc., containing such a request, that communication should be considered an attempted e-fraud, and the IT Manager should be informed immediately without responding.

3.3. If a user discovers that their password has been accidentally or otherwise disclosed, they must change their password immediately and inform the IT Manager promptly.

3.4. Users must ensure that others cannot see their screens when typing their login password, and should not position their screens in a way that allows anyone, including colleagues, to see them entering their password. Screens should also be placed within the office in a way that prevents them from being seen from outside the building.

3.5. Users should not enter their passwords on a website unless they are certain that it is the Company's official corporate information and communication systems/website. The best way to ensure this is to bookmark the sites yourself.

This involves providing your own URLs or accessing them using the URLs you have entered. Avoid using links, especially those in emails that claim to be legitimate.

4. CHANGING PASSWORDS

4.1. It is essential for users to change their passwords at regular intervals. The Deputy General Manager may determine the password change period to be between 30 days and one year, depending on the roles and responsibilities of the account holders authorized by the Company.

4.2. You can change your password by logging in to the computers registered in the company inventory and using the following link: http://www.kardelenboya.com.tr/

4.3. Reusing old passwords is not permitted. This is good practice, and you can apply it to systems outside the company as well.

4.4. Users whose passwords are found not to comply with the provisions of this Regulation will be immediately required to change their passwords.

4.5. Users who need to change their passwords will be contacted by a Company employee via email, phone, or in person. Users will then be able to change their passwords with the Company. He should not disclose this to anyone, including his staff.

5. PASSWORDS TO BE USED FOR EXTERNAL SYSTEMS

5.1. It is recommended that you apply the best use practices described in this Regulation when using other systems outside the Company.

5.2. Avoid using your existing username and password within the Company to create accounts on websites or other Internet resources.