ŞİFRE POLİTİKASI

1.0 AMAÇ

Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. İşbu politikanın amacı, Levent Kaya Otel İşletmeciliği bünyesinde bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkında standart oluşturmaktır.

2.0 KAPSAM

İşbu politika, Levent Kaya Otel İşletmeciliği'nde kullanıcı hesabı olan (bilgisayar ağına erişen ve şifre gerektiren kişiler) bütün kullanıcıları kapsamaktadır. Şirket çalışanları ve uzak noktalardan erişim sağlayanlar aşağıda belirtilen kurallar dâhilinde şifreleme yapmakla sorumludurlar.

3.0 POLİTİKA

3.1. Genel

a) Bütün sistem seviyeli şifreler (örnek, root, administrator) en az 3 ayda bir değiştirilmelidir.

b) Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web vs.) en az 6 ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her 4 ayda birdir.

c) Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.

d)Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

e)Kullanıcı, şifresini başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir.

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		

f) Şirket çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.

g) Bir kullanıcı adı ve şifresi birim zamanda birden çok bilgisayarda kullanılmamalıdır.

3.2. Ana Noktalar

A. Genel Şifre oluşturma Kuralları

Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri. Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.

Zayıf şifreler aşağıdaki karakteristiklere sahiptir:

a) Şifreler sekizden daha az karaktere sahiptir.

b) Şifreler sözlükte bulunan bir kelimeye sahiptir.

c) Şifreler aşağıdaki gibi ortak değere sahiptir.

- Ailesinin, arkadaşının sahip olduğu bir hayvanın veya bir sanatçının ismine sahiptir.
- Bilgisayar terminolojisi ve isimleri, komutlar, donanım veya yazılım gibi
- “bilişim” , “Ankara” , “İstanbul” gibi
- AaaBb, qwerty, qazwsx, 123321 gibi sıralı harf veya rakamlar

Güçlü şifreler ise aşağıdaki karakteristiklere sahiptir:

a) Küçük ve büyük karakterlere sahiptir (A-Z, a-z).

b) Hem dijit hemde noktalama karakterleri ve ayrıca harflere sahiptir(0-9, !, @, &, =, (, }, ?)

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		

c) En az sekiz adet alfanümerik karaktere sahiptir.

d) Herhangi bir dildeki argo lehçe veya teknik bir kelime olmamalıdır.

e) Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır.

B. Şifre Koruma Standartları

Emident Özel Sağlık Hizmetleri Ticaret Ltd. Şti. bünyesinde kullanılan şifreleri kurum dışında herhangi bir şekilde kullanmayınız. Kimse ile paylaşmayınız. İlgili şifreler Şirkete ait gizli bilgiler olarak düşünülmelidir. Değişik sistemler için farklı şifreleme kullanın.

a) Aşağıdakiler yapılmayacaklar listesidir.

- Herhangi bir kişiye telefonda şifre vermek
- E-posta mesajlarında şifre belirtmek
- Üst yöneticinize şifreleri söylemek
- Başkaları önünde şifreler hakkında konuşmak
- Aile isimlerini şifre olarak kullanmak
- Şifreleri işten uzakta olduğunuzda iş arkadaşlarınıza bildirmek

b) Uygulamalardaki "şifre hatırlatma" özelliklerini seçmeyiniz.

c) Şifreler en az 6 ayda bir değiştirilmelidir. Tavsiye edilen aralık ise 4 ayda birdir.

d) Şifrelerin değiştirilip değiştirilmediği yapılan testler ile takip edilir.

C. Uygulama Geliştirme Standartları

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		

ŞİFRE POLİTİKASI

Uygulama geliştiricileri programlarındaki aşağıdaki güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

a) Bireylerin (grupların değil) kimlik doğrulaması işlemini destekleyebilmelidir.

b) Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.

c) Kural yönetim sistemini desteklemelidir.

D. Uzaktan Erişen Kullanıcılar İçin Şifre Kullanımı

Şirketin bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir passpharase ile yapılacaktır.

E. Passpharase

a) Bir passpharase standart şifrelerden daha uzun karakter dizisine sahiptir. (Genellikle 4'ten 16' ya kadar karaktere sahiptir.), dijital imzaların (bir mesajı gönderen kişinin gerçekten o kişi olduğunu kanıtlayan kodlanmış bir imza), mesajların kodalanması veya çözülmesinde kullanılır.

b) Passpharase'ler şifreler gibi değildir. Passpharase şifrelerden daha uzundur, dolayısı ile daha güvenlidir.

c) Passpharase'ler tipik olarak birçok kelimeden ibarettir. Bundan dolayı passpharase'ler "sözlük" saldırılarına karşı daha güvenlidir.

d) İyi bir passpharase büyük ve küçük harf ve rakamlardan oluşan birleşime sahiptir. Örnek bir passpharase: "?*@102incicaddedekiTrafik*&#!#Busabah"

e) Şifreleme için geçerli olan bütün kurallar passpharaseler için de geçerlidir.

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		