1. **AMAÇ – KAPSAM:**

Personelin, bilgi sistemlerinin kullanımında güçlü şifreleme mekanizmalarını kullanması, oluşturulan şifrelerin korunması ve bu şifrelerin değiştirilme sıklığı hakkında standart oluşturmaktır.

Firma ve hizmet verdiğimiz kurumlar kapsam dâhilindedir.

1. **SORUMLULAR:**

Bu prosedürün oluşturulmasından Bilgi İşlem Müdürü sorumlu olup kullanıcı hesabı olan (şifre gerektiren kişiler uygulamalara erişen) bütün çalışanlar da uygulamadan sorumludur.

1. **UYGULAMA:**

Şifreleme, bilgi güvenliğinin sağlanması açısından kritik bir öneme sahip olup kullanıcı hesaplarında ilk güvenlik katmanını teşkil etmektedir. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. Firma personeli ve uzak noktalardan erişenler aşağıda belirtilen kurallar dahilinde şifreleme yapmakla sorumludurlar.

 **Genel Kurallar**

1. Bütün sistem seviyeli şifreler (örnek, root, administrator, enable, vs) en az üç ayda bir değiştirilmelidir.
2. Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her dört ayda birdir.
3. Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.
4. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
5. Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara yada elektronik ortamlara yazmaması konusunda eğitilmelidir.
6. Firma çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.
7. Bir kullanıcı adı ve şifresinin birim zamanda birden çok bilgisayarda kullanılmamalıdır.
8. SNMP kullanıldığı durumlarda varsayılan olarak gelen “public”, “system” ve “private” gibi community string’lere farklı değerler atanmalıdır.
9. Ortak kullanım alanlarında bulunan yazıcılardan alınacak çıktılar şifre korumalı olarak gönderilmelidir.

**Şifre Oluşturma Kuralları:**

Kullanıcılar, domain erişimlerinde, web uygulamalarında, e-posta hesaplarında, ekran koruma işlemlerinde, network erişim uygulamalarında vb. şifreleme mekanizmaları kullanılmaktadırlar. Bu yüzden bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermesi gerekli olup bütün kullanıcı ve sistem seviyeli şifrelemeler aşağıdaki kuralları uygulamalıdır.

**Zayıf Şifreler:**

Zayıf şifreler aşağıdaki karakteristiklere sahip olup kullanıcılar bu tip şifrelemeden kaçınmalıdır.

1. Şifreler sekizden daha az karaktere sahiptirler.
2. Şifreler sözlükte bulunan bir kelimeye sahip değildir.
3. Şifreler aşağıdaki gibi ortak değere sahiptir.
	* Harf ve rakamlardan karmaşık oluşur.
	* Bilgisayar terminolojisi ve isimleri; komutlar, siteler, şirketler, donanım, yazılım vb.
	* ”Verita”, ”trabzon”, ”ankara” gibi özel isimler.
	* Doğum tarihi, adres ve telefon numaraları gibi kişisel bilgiler.
	* Aaabbb, qwerty,zyxwuts, 123321 vs. Gibi sıralı harf veya rakamlar.
	* Yukardaki herhangi bir kelimenin geri yazılış şekli.
	* Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi (örnek, gizli1, gizli2).

**Güçlü Şifreler:**

Güçlü şifreler aşağıdaki karakteristiklere sahip olup kullanıcılar bu tip şifreleme kurallarını uygulamalıdır

1. Küçük ve büyük karakterlere sahiptir (örnek, a-z, A-Z)
2. Hem dijit hemde noktalama karakterleri ve ayrıca harflere sahiptir. (0-9, !@#$%^&\*()\_+|~-=\`{}[]:";'<>?,./)
3. En az altı adet alfa nümerik karaktere sahiptir.
4. Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
5. Aile isimleri gibi kişisel bilgilere ait olmamalıdır.
6. Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır. Kolayca hatırlanabilen şifreler oluşturulmalıdır. Örnek olarak; ”Birinci kalite hedefimiz müşteri memnuniyetinin sağlanmasıdır” ”1KhMmS!” veya türevleri şeklinde olabilir.

Not: Yukarıdaki herhangi bir örneği şifre olarak kullanmayınız.

**Şifre Koruma Standartları:**

Bütün kullanıcılar aşağıdaki kurallara titizlikle uymalıdır.

1. Firma bünyesinde kullanılan şifreler firma dışında herhangi bir şekilde kullanmamalıdır. (örnek, internet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde).
2. Değişik sistemler için farklı şifreleme kullanılmalıdır. Örnek, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre.
3. Firma bünyesinde kullanılan şifreleri herhangi bir kimseyle paylaşmayınız. Bütün şifreler firmaya ait gizli bilgiler olarak düşünülmelidir.
4. Herhangi bir kişiye telefonda şifre verilmemelidir.
5. e-posta mesajlarında şifre belirtmemelidir.
6. Üst yönetici dahil hiç kimseye şifre söylenmemelidir.
7. Başkaları önünde şifreler hakkında konuşulmamalıdır.
8. Aile isimlerini şifre olarak kullanılmamalıdır.
9. Herhangi form üzerinde şifre belirtilmemelidir.
10. Şifreler aile bireyleri ile paylaşılmamalıdır.
11. Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza söylenmemelidir.
12. Herhangi bir kimse şifre isteğinde bulunursa bu dokümanı referans göstermesini ve ilgili amirini aramasını söyleyiniz.
13. Uygulamalardaki “şifre hatırlama” özelliklerini seçmeyiniz. (örnek, Outlook, Internet Explorer vs.)
14. Şifreleri herhangi bir yere yazmayınız ve herhangi bir ortamda elektronik olarak saklamayınız.
15. Şifreler an az altı ayda bir değiştirilmelidir (sistemlerin şifreleri ise en az üç ayda bir değiştirilmelidir). Tavsiye edilen aralık ise 3 ayda birdir.
16. Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

**Güçlü Şifre Kullanımı:**

Passphrase, şifreler ile benzer prensiplere sahiptir. Passphraseler, şifrelerden daha uzundur, dolayısı ile daha güvenlidir. Passphrase’ler tipik olarak birçok kelimeden ibarettir. Bundan dolayı passphrase’ler “sözlük” saldırılarına karşı daha güvenlidir. Passpharese’ler güçlü şifreleme oluşturulmasında ve PKI altyapılarında kullanılmalıdır.

1. Bir passphrase 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 kodlanması veya çözülmesinde kullanılır.
2. İyi bir passphrase büyük ve küçük harf ve rakamlardan oluşan kombinasyona sahiptir. Örnek bir passphrase: "\*?#>\*@1012inciCaddekiTrafik\*&#!#BuSabah"
3. Şifreleme için geçerli olan bütün kurallar passphrase’ler için de geçerlidir.

1. **İLGİLİ DOKÜMANLAR**