1. SORUMLULAR:

Bu talimatın uygulamasından İÜ kullanıcıları sorumludur.

2. TANIMLAR

İÜ: İstanbul Üniversitesi
BİDB: Bilgi İşlem Daire Başkanlığı

3. UYGULAMA

- **Parola Oluşturma Kuralları (Genel)**

- Parolalar en az 8 karakter uzunluğunda olmalıdır ve bu karakterlerin en az 3 tanesi sayılardan oluşmalıdır.
- Aşağıdaki karakterlerin en az üçünü içermelidir;
  - Büyük harf, (örn. ABCDEF...)
  - Küçük harf, (örn, abcdef ...)
  - Rakam, (örn: 1234567890)
  - Noktalama işareti, (örn: !?., vb.)
  - Özel karakterler (Örn: @#$%^&*()_+|~-=\`{}[]:";'<>/ vb.)

- Parolalar aşağıdaki şekilde oluşturulmamalıdır;

  - İçeriğinde, kişisel bilgiler bulunmamalıdır (örneğin aile bireylerinin isimleri, doğum tarihleri, telefon numarası veya adres bilgileri gibi)
  - Kelime veya rakam dizileri kullanılmamalıdır. (Örn; aaabbb, qwerty, zyxwvuts, 12345678, 123321, vb.)

- **Parola Oluşturma Kuralları (Sistem)**

  - Tüm kullanıcı hesaplarına ait bir parola vardır.
  - Yeni kullanıcı hesaplarına ait parolaların ilk kez giriş yapılırken kullanıcı tarafından kurallara uygun olarak tanımlanması gerekmektedir.
  - Başarısız parola denemeleri üst üste 3 kere ile sınırlandırılmıştır. Üçüncü denemeden sonra şifre ve bağlı olduğu kullanıcı, kullanım dışı bırakılmalıdır. Yenilenmesi / kullanım dışılığın açılması için ilgili sistemin yöneticisine telefonla başvurması ve kendisine sorulan (TC kimlik, kurum sicil vb.) sorulara cevap vermesi beklenir.
  - Aynı parola ile birden fazla cihaz üzerinden sisteme giriş yapılmasına izin verilmez.
  - Kullanıcılar giriş yaptıkları bilgisayardan çıktıktan sonra farklı bir bilgisayardan giriş yapabilirler.

- Yazılan parolanın ekranda görünmemesi veya maskelenerek görünmesi sağlanır.
- Kullanıcı parolaları, saklandıkları ortamlarda, geri dönüşü mümkün olmayan bir şekilde bozularak korunur (örneğin Hash), bu sayede en yetkili kişilerin bile kullanıcı parolasını görmesi engellenmelidir.
- Bilgi kaynaklarına başarılı ve başarısız erişimlerin tarih, zaman ve erişilen kaynağın detayı ile ilgili bilgilerinin kaydı tutulmalıdır.
- Kullanıcıların kimlik doğrulaması yaparak oturum açtıkları sistemlerin başından ayrıldıklarında (sisteme parola ile giriş yapıldıktan sonra sistem açık bırakılması halinde) en geç 10 dakika sonra otomatik olarak kapanması (sistemin kilitlenmesi) sağlanmalıdır.
- Halka açık veya paylaşılan ağlardan iletilen kimlik bilgileri güçlü şifreleme metotları ile (SSL) korunmalıdır.
- Başkaları tarafından öğrenildiğinden şüphelenilen parolalar hemen değiştirilmelidir.
- Kullanıcılar parolalarını 6 ay içinde kullanmamaları durumunda ilgili hesap dondurulmalıdır.
- Kritik kaynaklara 3'lü şifre ile erişilebilir, bu sayede tek bir kullanıcının sistemde güvenlik ihlali oluşturmasına izin verilmemelidir. (örneğin bilgi kaynaklarına erişim kayıtları gibi kayıtlara en yetkili kullanıcı bile tek başına erişemez, bu yetkili kullanıcılardan 3 kişinin oluşturduğu bir heyet kendi şifrelerini aynı anda girerek kritik bilgilere erişebilir)

- **Parola Kullanım Kuralları**

- Parolalar en geç 3 ayda bir değiştirilmelidir.
- Her yeni parola için, son kullanılan 3 paroladan farklı yeni bir parola kullanılmalıdır.
- Parolalar hiç kimse ile paylaşılmamalıdır.
- Parolaların klavyeden girilmesi sırasında dikkatli olunmalı ve çevredeki kişilerin görmesine izin vermeyecek şekilde girilmelidir.
- E-posta yoluyla parolaların onaylanması veya güncellenmesi istenmez, bu yönde gelen e-postalar dikkate alınmamalıdır.
- Herhangi bir kullanıcının parolası bilerek veya bilmeyerek bir kişi tarafından öğrenilirse, ilgili kullanıcı uyarılmalıdır. Gerekirse zarar verme ihtimaline karşı parolanın kullanıldığı sistem yöneticisi uyarılmalıdır.
- Aynı parola birden fazla kaynakta kullanılmamalıdır.
- Parolalar ilave bir şifreleme metodu kullanılmadan hatırlamak amacıyla kayıt edilmemelidir (kâğıt, bilgisayardaki bir dosya, cep telefonu gibi ortamlarda saklanmamalıdır).
- İnternet tarayıcılarında (internet explorer, chrome, firefox vb.) "Parolayı hatırla" seçeneğinin kişisel bilgisayarlar dışında kullanılması yasaktır, kişisel bilgisayarlarda ise bir güvenlik açığı olduğu hatırlanmalıdır.

- **Parolanın Unutulması**

- Bütün sistemler üzerinde, kullanıcıların parolasını unutma ihtimaline karşı bir çözüm sunulmalıdır.
- Bu çözüm, kullanıcıların kişisel doğrulamasını yapmak amacıyla kişilerin gizli soruları ve özlük bilgilerinden oluşan en az iki soru içermelidir.
- Hiçbir kullanıcının parolası güvenlik yöneticisinin onayı olmadan diğer yetkili kişiler tarafından değiştirilmemelidir.
- Bütün parola değiştirme ve güncelleme işlemleri ayrıca kayıt altına alınmalı kullanıcı, eski ve yeni parolanın bozulmuş hali, değiştiren kişi (kullanıcıdan farklıysa) değiştirme saat ve tarihi, 3'lü şifre ile korunmalıdır.

4. İLGİLİ DOKÜMANLAR

-