BGYS POLİTİKASI

Politika Numarası	PLTK-11
Politika Tanımı	Kimlik Doğrulama Politikası
Amaç ve İlkeler	Kimlik doğrulamanın uygun bir şekilde sağlanması ve kimlik doğrulama süreçlerindeki başarısızlıkların önlenmesidir.
Sorumluluklar	**Bilgi İşlem Personeli:** Kimlik doğrulama işlemlerine yönelik sistem kurulması ve denetlenmesinden sorumludur. **Kullanıcılar**: Bu politikanın şartlarına uygun hareket etmekten sorumludur.
Sapma ve Özel Durumlar	Bu politikanın ihlali, disiplin önlemlerine neden olabilir.

UYGULAMA

Kimlik doğrulama bilgilerinin tahsisi ve yönetimi şu şekilde sağlanmalıdır:

a) Tahmin Edilemez ve Benzersiz Kimlik Bilgileri: Kayıt işlemleri sırasında otomatik olarak oluşturulan geçici gizli kimlik doğrulama bilgileri, tahmin edilemez ve her bir kullanıcı için benzersiz şekilde oluşturulmalıdır. Kullanıcılar bu geçici bilgileri ilk kullanımdan sonra değiştirmek zorundadır.

b) Kimlik Doğrulama İşlemleri: Yeni, ikame veya geçici kimlik doğrulama bilgilerinin sağlanması öncesinde, kullanıcının kimliğini doğrulamak için kurallar belirlenmelidir.

c) Güvenli İletişim Kanalları: Kimlik doğrulama bilgileri, güvenli kanallar aracılığıyla (örneğin, kimliği doğrulanmış ve korumalı bir kanal üzerinden) kullanıcılara iletilmelidir. Korumasız elektronik iletişim yöntemleri, özellikle açık metin içeren e-posta mesajları kullanılmaz.

d) Kullanıcı Onayı: Kullanıcılar, kimlik doğrulama bilgilerini aldıklarında bu durumu onaylamalıdır.

e) Varsayılan Bilgilerin Değiştirilmesi: Tedarikçiler tarafından önceden tanımlanmış veya varsayılan kimlik doğrulama bilgileri, sistem veya yazılım kurulumunun hemen ardından değiştirilmelidir.

f) Olay Kayıtlarının Tutulması ve Gizliliği: Kimlik doğrulama bilgilerinin tahsisi ve yönetimi ile ilgili tüm önemli olaylar kayıt altına alınmalı ve bu kayıtların gizliliği sağlanmalıdır. Kayıt tutma yöntemleri, onaylı bir parola koruma ve yönetim aracı kullanılarak belirlenmelidir.

Kimlik doğrulama bilgilerine erişimi olan veya bunları kullanan her kişinin aşağıdaki uygulamaları takip etmesi tavsiye edilmektedir:

a) Gizliliğin Korunması: Parolalar gibi gizli kimlik doğrulama bilgileri kesinlikle gizli tutulmalıdır. Kişisel gizli kimlik doğrulama bilgileri hiçbir koşulda başkalarıyla paylaşılmamalıdır. Birden çok kullanıcıya bağlı veya kişisel olmayan öğelere bağlı kimliklerin gizli bilgileri, sadece yetkili kişilerle paylaşılmalıdır.

b) Hızlı Müdahale: Eğer etkilenmiş veya güvenliği ihlal edilmiş kimlik doğrulama bilgileri tespit edilirse, derhal bir uyarı yapılmalı ve bu bilgiler hemen değiştirilmelidir.

c) Güçlü Parolaların Seçilmesi: Parola kullanımı gerektiğinde, en güvenli uygulamalara uygun güçlü parolalar seçilmelidir. Bu parolalar:

- ⇒ Tahmin edilmesi kolay olmamalı ve kişiyle ilgili bilgilere dayanmamalıdır.
- ⇒ Sözlükte bulunan kelimeler veya bunların kombinasyonları içermemelidir.
- ⇒ Alfanümerik ve özel karakterler içermeli ve hatırlaması kolay olmalıdır.
- ⇒ Minimum bir uzunluğa sahip olmalıdır.

d) Farklı Parolaların Kullanılması: Farklı hizmetlerde ve sistemlerde aynı parolaların kullanılması kesinlikle önerilmez.

e) Kurallara Uyum: Bu kurallara uyma yükümlülüğü, firmamızın istihdam hüküm ve koşullarına dahil edilmiştir.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
20.04.2018	01/26.01.2024	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

Parola yönetim sistemi şu prensiplere dayanmalıdır:

a) Kullanıcı Kontrolü: Kullanıcıların kendi parolalarını seçmelerine ve düzenli olarak değiştirmelerine izin verilir. Ayrıca, giriş hatalarını düzeltmek için bir onay işlemi bulunmalıdır.

b) Güçlü Parolaların Uygulanması: Kullanıcıların seçtiği parolalar, güçlü parola kriterlerine uygun olmalıdır.

c) İlk Girişte Parola Değişimi: Kullanıcılar, ilk girişlerinde parolalarını değiştirmeye zorlanmalıdır.

d) Zorunlu Parola Değişiklikleri: Güvenlik ihlali durumunda veya iş akdi sona eren bir kullanıcının kimlikleri aktif olarak kullanılmaya devam ediyorsa veya paylaşılan kimlikler varsa, parola değişiklikleri zorunlu kılınmalıdır.

e) Tekrar Kullanımın Önlenmesi: Önceki parolaların tekrar kullanılması engellenmelidir.

f) Güvenlik Kontrolleri: Yaygın olarak kullanılan parolaların veya güvenlik ihlaline uğramış kullanıcı adı-parola kombinasyonlarının kullanılması engellenmelidir.

g) Parolaların Gizliliği: Parolaların girilirken ekranda gösterilmemesi sağlanmalıdır.

h) Parolaların Güvenli Saklanması ve İletilmesi: Parolalar, korumalı bir biçimde saklanmalı ve iletilmelidir.

Parola şifreleme ve hesaba dayalı adresleme, onaylanmış kriptografik tekniklere uygun olarak gerçekleştirilmelidir. Bu yöntemler, parolaların güvenliğini ve gizliliğini sağlamak için titizlikle uygulanmalıdır.