MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

PAROLA POLİTİKASI

İçindekiler

1. Amaç

Bu doküman, "BGYS Kapsam Analizi Dokümanı"nda belirtilen, kuruluşumuz birimlerinde kullanılan parolalarının yönetimi için gereken kuralları tanımlamak amacıyla oluşturulmuştur.

2. Kapsam

Bu doküman, "BGYS Kapsam Analizi Dokümanı"nda belirtilen, kuruluşumuz birimlerinde kullanılan tüm parolaları kapsar.

3. Sorumluluk

Rol/Unvan / Görev	Üst Yönetim	Üst Yönetim Temsilcisi	BGYS Yöneticisi	BGYS Ekip Üyeleri	Diğer Çalışanlar
Dokümanın Hazırlanması			X	X	
Dokümanın Kontrolü			X	X	
Dokümanın Onaylanması	X	X			
Dokümanın Yayınlanması			X		
Dokümanın Güncellenmesi			X		
Dokümanın Uygulanması	X	X	X	X	X
Dokümanın Uygulamadan Kaldırılması	X	X			

4. Tanımlar ve Kısaltmalar

Terim	Tanım/Açıklama
Aktif Dizin Etki Alanı	Bünyesinde kullanıcılar, gruplar ve yapılandırma bilgileri gibi pek çok öğeyi ve kimlik doğrulama, yetkilendirme gibi özellikleri barındıran yapı.
BGYS	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
Politika	Bir şirket, kurum veya kişinin görüş, felsefe, amaç ve tutumunun belirli şekilde ifadesini, bu görüş, felsefe veya amaç doğrultusunda bir hareket planını içeren doküman tipidir.

5. Parola Politikası

Parolalar, kurumun bilgilerini korumak için uygulanan en önemli güvenlik önlemidir. Bu yüzden kolay tahmin edilemeyen ve güvenlik gerekliliklerini karşılayacak şekilde bir parola belirlenmelidir. Parolalar kuruluşumuzda çeşitli amaçlar için kullanılmaktadır. Parola kullanım amaçlarından bazıları şunlardır: Kullanıcı hesapları, web hesapları, e-posta hesapları, router/switch local girişi vb. Bu bağlamda tüm kullanıcılar, güçlü parola belirleme kurallarını bilmelidir. Parola belirlerken dikkat edilmesi gereken hususlar aşağıda tanımlanmıştır:

(1) Kullanıcılar, kendilerine verilmiş olan kullanıcı adlarına ait parolalarını başkaları ile paylaşmaz ve korurlar. Aksi durumlarda oluşabilecek olumsuz olaylardan kullanıcının kendisi sorumlu olacaktır.
(2) Kullanıcılar parolalarını 180 günde bir değiştirmelidirler. Parolanın çalınması ihtimali olduğunda bu süre beklenmeden parola değiştirilir. Parolalar aşağıda belirtilen özelliklere göre oluşturulur:
(1) Kullanıcılar, en az 8 karakter uzunluğunda, büyük harf, küçük harf, özel karakter ve rakam içeren, güçlü ve karmaşık parolalar belirlemelidir.
(2) Parolalar; doğum tarihi, adres veya telefon numaraları gibi kişisel bilgilerden oluşturulmaz.
(3) Parolalar; sıralı harf veya rakamlardan oluşturulmaz.
(3) Kullanıcıya verilen ilk parola ile parolasını unuttuğu zaman verilen parola "geçici parola" olarak düşünülür ve ilk oturum açılışında değiştirilir. Kullanıcılara verilen geçici parolalar birbirinden farklı olmalıdır.
(4) Kullanıcılar son kullandıkları 3 parolayı, parola yenileme esnasında kullanamaz.
(5) Parola sıfırlama talepleri EBYS üzerinden iletilir.
(6) Kurum personeli şahsi parolalarını özel kontrol altında tutar, parolalarını Bilgi İşlem Birimi personeli de dâhil olmak üzere hiç kimseyle paylaşmaz.
(7) Kullanıcılar, parolalarının ele geçirildiğinden kuşkulandıklarında parolasını değiştirir, Bilgi İşlem Birimi'ne haber vererek gerekli ise bilgi güvenliği ihlal olayı kaydı açılmasını sağlar.
(8) Kullanıcılar, kurum hizmetleri için kullandıkları parolaları, sosyal medya, bankacılık, alışveriş web site vb. üyeliklerinde kullanamaz.
(9) Parolalar, dosya, otomatik komut dosyası, yazılım makrosu, erişim kontrolü olmayan bilgisayarlar ve başkalarının fark edebileceği şekilde bilgisayar donanımlarının fiziksel dış alanlarına, not kağıtlarına yazılmaz, başkalarının görebileceği şekilde herhangi bir panoya asılmaz.
(10) Sistemlere giriş ekranlarında herhangi bir ipucu olamaz. Eğer böyle bir işlem adımı var ise parola hatırlatması yapılmaz ve kullanıcıya geçici parola verilir. Hesabın bloke olması ya da parolanın unutulması durumlarında Bilgi İşlem Birimi'ne başvurulur.
(11) Bütün sistemler, sisteme giriş anında kullanıcı adı ya da parolanın yanlış olması durumunda hangisinin yanlış olduğuna dair bilgi mesajı vermez.

(12) Başarısız parola denemeleri sınırlandırılmıştır. Belirli sayıdaki hatalı denemeden sonra kullanıcıya ait istek yapan IP belirli süre bloklanır. (E-posta tarafında).
(13) Sunuculara, sistemlere, yazılımlara, veri tabanlarına ve ağ cihazlarına erişim sağlayan kullanıcı hesapları, etki alanı parola kriterlerine ek olarak en az aşağıdaki özelliklerde olmalıdır:

(a) Parolalar, en az 8 karakterden oluşur ve büyük harf, küçük harf, alfa numerik ve rakam özelliklerinin hepsini içerecek şekilde karmaşık olarak belirlenir.
(b) Teknik olarak desteklenmeleri durumunda Root ve Administrator kullanıcı adı haricinde ayrı bir kullanıcı adı ile bağlanılır. (BSD tarafında)
(14) Gerçek kişilere ait olmayan kurumsal e-posta hesaplarının erişim yetkisi ilgili birim yöneticisine veya onun belirlediği personele verilir. İlgili e-posta hesabının parola işlemleri ve erişim bilgileri erişim yetkisi verilen personelin sorumluluğundadır.
(15) Kurumsal bilgiye erişilebilen mobil cihazlar için ekran kilidi kullanımı zorunludur. Ekran kilidini açmak için kolay tahmin edilemeyen PIN kodu, parola veya desen kullanılır.
(16) Kurumda e-imza cihazı için kullanılan PIN kodları;
(a) Doğum tarihi, kimlik numarası veya telefon numaraları gibi kişisel bilgilerden oluşturulamaz.
(b) Birbirini tekrarlayan ve ardışık rakamlardan oluşturulamaz.
(c) PIN kodu e-imza üzerine yazılamaz.

6. İlgili Dokümanlar

6.1. İç Kaynaklı Dokümanlar

(1) KA.01 BGYS Kapsam Analizi

6.2. Dış Kaynaklı Dokümanlar

(1) TS ISO/IEC 27001:2013 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					