Revizyon İzleme Tablosu		
Rev. No	**Rev. Tarihi**	**Açıklama**
00	-	İlk Yayın

1. AMAÇ

Bu politikanın amacı Bilecik Şeyh Edebali Üniversitesi Bilgi İşlem Daire Başkanlığı ağ ve erişim güvenliği kapsamında e-posta, parola, ağ erişim,sunucu,uzak bağlantı,kablosuz ağ güvenliğine yönelik kurallarını belirlemek amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika Bilgi İşlem Daire Başkanlığı tarafından sunulan hizmetlerde e-posta, parola, ağ erişim,sunucu,uzak bağlantı,kablosuz ağ güvenliğinde izlenecek kuralları içermektedir ve bütün çalışanları kapsamaktadır.

3. UYGULAMA

- Varlık ve süreç sahipleri, kendi varlıkları veya süreçlerine yönelik bilgi güvenliği risklerini yansıtan kontrolleri, erişim kontrol kurallarını, erişim haklarını ve kısıtlamalarına dair yetkilendirmelerden sorumludur.
- Erişim talepleri için Elektronik Belge Yönetim Sisteminde bulunan Bilgi İşlem İş Talep Formu doldurularak BİDB' ye istek iletilir.
- BİDB uygun olan talepleri gerçekleştirir ve geri bildirimde bulunur.
- Kurum dışından Kurumun bilgi ağı servislerine yapılacak bağlantılar, yetkisiz erişimlere izin vermeyecek şekilde denetlenir ve kontrol altına alınır. Buna ilişkin kurallar BGYS. PLT. 02 Ağ ve Erişim Güvenliği Politikasında belirtilmiştir.
- Sistemlerde kimlik doğrulama için kullanılan parolalar, ilk başarılı kimlik doğrulamanın sonrasında kullanıcıların sadece kendi bildikleri parolalarla değiştirilir ve BGYS.PLT.03 Parola (Şifre) Güvenliği Politikasına uygun olarak belirlenir.
- Kişisel verilerin anonim hale getirilmesi BŞEÜ-Kişisel Verileri Saklama ve İmha Politikası çerçevesinde belirlenmiş ve uygulanmaktadır.
- Kişisel verilerin bulunduğu bilişim sistemleri belirlenmiştir. Bilişim sistemlerine ait kullanıcı rolleri ve erişim yetkilerini açıklayan matris BİDB bulut sistemimiz üzerinde tanımlanmış ve takip edilmektedir.
- Kullanıcı hesapları ve parolaları başkalarıyla paylaşılmaz. Kullanıcı hesabıyla yapılan tüm işlemlerden kullanıcı hesabı sahibi sorumludur.
- Kurumda görev değiştiren kullanıcının erişim hakları iş gereksinimlerine göre yeniden düzenlenir.
- Kullanıcı hesapları, ilgili sistem sorumluları tarafından belirli aralıklarla kontrol edilip tespit edilmektedir. 6 ay boyunca kullanılmayan hesaplar, yönetici onayı alınarak pasif duruma getirilir / silinir.
- Kurumla ilişiği kesilen personelin ve geçici kullanıcıların (geçici görevli, stajyer vb.) kullanıcı hesapları ilişiği kesildiği an itibarı ile devre dışı bırakılır.
- Yönetim için sunuculara sağlanan erişimde "yönetici (admin/root)" yetkisi sadece sorumlu personele verilir.

4. İLGİLİ DÖKÜMANLAR

- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi 4.1.3.4 Maddesi
- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi 3.2.1.12 Maddesi