ERİŞİM KONTROL POLİTİKASI

1. Amaç

Bu Politikanın amacı; Sakarya Üniversitesi ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamındaki bilgi sistemlerine erişimlerin gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda yönetilmesine ilişkin temel prensipleri belirlemektir.

2. Kapsam

Bu politika; BGYS kapsamında Bilgi İşlem Daire Başkanlığı (BİDB), Bilgisayar Araştırma ve Uygulama Merkezi (BAUM) ve Uzaktan Eğitim Araştırma ve Uygulama Merkezi (UZEM) tarafından işletilen bilgi sistemleri, uygulamalar, ağ altyapısı ile fiziksel/dijital erişim noktalarına erişim yetkisi bulunan kullanıcıları (akademik/idari personel, öğrenciler, stajyerler, taşeron çalışanlar ve üçüncü taraflar) kapsar.

3. Sorumluluklar

3.1 Üst Yönetim

- Erişim kontrolüne ilişkin kurumsal çerçevenin oluşturulmasını ve uygulanmasını destekler.
- Bilgi Güvenliği Yönetim Sistemi kapsamında erişim kontrolünün etkin yürütülmesi için gerekli kaynakları sağlar.

3.2 Bilgi İşlem Daire Başkanlığı (BİDB), Bilgisayar Araştırma ve Uygulama Merkezi (BAUM) ve Uzaktan Eğitim Araştırma ve Uygulama Merkezi (UZEM)

- Sorumluluk alanlarındaki bilgi sistemleri, uygulamalar ve altyapılar üzerinde erişim kontrol mekanizmalarının uygulanmasını sağlar.
- Kullanıcı ve ayrıcalıklı erişimlerin görev ve yetki esasına göre tanımlanmasını, güncellenmesini ve kaldırılmasını yürütür.
- Erişim faaliyetlerinin kayıt altına alınmasını ve ilgili prosedürler doğrultusunda izlenmesini temin eder.

3.3 Bilgi Güvenliği Yönetim Sistemi (BGYS) Ekibi

- Bu politikanın ISO/IEC 27001 standardı ile uyumunu izler.
- Politikanın gözden geçirilmesi ve gerekli güncellemelerin yapılması sürecini koordine eder.

3.4 Birim Yöneticileri

- Personelin erişim taleplerini görev ve sorumlulukları doğrultusunda değerlendirir ve onaylar.
- Görev değişikliği, geçici görevlendirme veya işten ayrılma durumlarını ilgili teknik birimlere zamanında bildirir.
- Sorumluluk alanındaki erişimlerin gerekliliğini periyodik olarak gözden geçirir.

3.5 Kullanıcılar

- Kendilerine tahsis edilen erişim haklarını yalnızca görev kapsamı içinde kullanmakla yükümlüdür.
- Kimlik doğrulama bilgilerini korumak ve yetkisiz erişim şüphesi durumunda bildirimde bulunmakla sorumludur.
- Bu politika ile ilişkili prosedür ve rehberlerde belirtilen kurallara uyar.

3.6 Üçüncü Taraflar ve Tedarikçiler

- Kurum bilgi sistemlerine erişim sağladıkları durumlarda bu politika, ilgili sözleşmeler ve taahhütnameler kapsamında belirlenen kurallara uymakla yükümlüdür.
- Erişimlerini iş kapsamı ve sözleşme süresi ile sınırlı olarak kullanır.
- İş ilişkisi sona erdiğinde erişim haklarının kaldırılması süreçlerinde Üniversite ile iş birliği yapar.

4. Politika İlkeleri

- Bu politika kapsamındaki erişim süreçlerinin uygulanması ve kayıt altına alınması esasları, **Erişim Kontrol Prosedürü** ile güvence altına alınır.

4.1 Kimlik Doğrulama ve Yetkilendirme

- Bilgi sistemlerine erişim; kimlik doğrulama ve yetkilendirme mekanizmaları aracılığıyla sağlanır.
- Erişim yetkileri; **asgari yetki** ve **bilmesi gereken** prensipleri doğrultusunda, yalnızca görev tanımı kapsamında gerekli olan haklarla sınırlandırılarak tanımlanır.
- Çok faktörlü kimlik doğrulama (MFA) uygulamaları; teknik altyapı uygunluğu ve risk değerlendirme sonuçları dikkate alınarak planlanır ve uygulanır.

4.2 Hesap Yönetimi

- Kullanıcı hesapları yalnızca tanımlı başvuru ve onay süreçleri ile açılır.
- Üçüncü taraf hesapları sözleşme süresi ile sınırlıdır.
- Görev değişikliği veya ayrılış durumunda erişimler iptal edilir.

4.3 Güvenli Parola ve Oturum Yönetimi

- Parolalar **"Güçlü Parola İlkeleri"**ne uygun olarak oluşturulur.
- Varsayılan parolalar kalıcı olarak kullanılamaz.
- Parolalar en geç 6 ayda bir değiştirilir.
- Üst üste 5 hatalı girişte hesap kilitlenir.
- BGYS kapsamındaki bilgi sistemlerinde oturum güvenliği, otomatik kilitleme ve zaman aşımı mekanizmaları ile sağlanır.

4.4 Ayrıcalıklı Erişimlerin Sınırlandırılması

- Ayrıcalıklı hesaplar yalnızca yetkili teknik personele tanımlanır.
- Ayrıcalıklı erişimler süre ve kapsam ile sınırlandırılır.
- Ayrıcalıklı erişimler periyodik olarak gözden geçirilir.
- Ayrıcalıklı hesap parolaları yüksek gizlilik seviyesinde korunur.

4.5 Bilgi Güvenliği ve Sınıflandırma

- Bilgiye erişim, bilgi sınıflandırma seviyeleri ve gizlilik derecelerine uygun şekilde sağlanır.
- Hassas ve gizli bilgiler için ek erişim ve izleme kontrolleri uygulanır.
- Hassas verilerin işlendiği ortamlarda, veri maskeleme veya benzeri veri koruma teknikleri, uygulanabilir olduğu durumlarda, erişim kontrolü ilkeleri ve iş gereklilikleri doğrultusunda uygulanır.

4.6 Fiziksel Erişim Kontrolleri

- Sunucu odaları ve kritik alanlara erişim yetkilendirilmiş personel ile sınırlıdır.
- Fiziksel erişim yetkileri görev gerekliliğine dayanır ve kayıt altına alınır.
- Fiziksel erişim koşulları **Fiziksel ve Çevresel Güvenlik Prosedürü** ile uyumlu yürütülür.

4.7 Kaynak Koduna ve Geliştirme Ortamlarına Erişim

- Üniversiteye ait yazılım projelerinin kaynak kodlarına erişim, yalnızca yetkilendirilmiş kişilerle sınırlıdır.
- Erişimler kayıt altına alınır ve izlenebilir şekilde yürütülür.

4.8 Görevlerin Ayrılığı

- Erişim talebi, onay, uygulama ve izleme süreçleri ayrıştırılmıştır.
- Log kayıtlarının bütünlüğü korunur; sistem yöneticileri log kayıtlarını değiştirme veya silme yetkisine sahip değildir.
- İzleme ve denetim faaliyetleri **Log Yönetimi ve İzleme Prosedürü** kapsamında yürütülür.

4.9 Mevzuat ve Yükümlülükler

- Erişim hakları, yürürlükteki mevzuat, sözleşmeler ve ilgili yönetmeliklere uygun şekilde yönetilir.
- Üçüncü taraflar erişim öncesinde **Gizlilik ve Bilgi Güvenliği Taahhütnamesi** imzalar.

4.10 Bilgi Güvenliği Olay Yönetimi

- Erişimle ilgili güvenlik olayları (ör. parola ihlali, yetkisiz erişim, ayrıcalıklı hesap kötüye kullanımı) derhal Bilgi İşlem Daire Başkanlığı (BİDB)'na bildirilir.
- Bu olaylar **Bilgi Güvenliği Olay Yönetimi Prosedürü** kapsamında değerlendirilir ve gerekli önlemler alınır.

5. Politikanın İhlali

Politikaya aykırı davranışlar disiplin yönetmelikleri ve ilgili mevzuat çerçevesinde yaptırımlara tabidir. Yetkisiz erişimler derhal askıya alınır ve ilgili olay **Bilgi Güvenliği Olay Yönetimi Prosedürü** kapsamında değerlendirilir.

6. Politikanın Gözden Geçirilmesi

Bu politika, teknolojik gelişmeler, mevzuat değişiklikleri ve Üniversitemizin ihtiyaçları doğrultusunda yılda en az bir kez gözden geçirilir ve güncellenir.