1. AMAÇ

OSTİM Teknik Üniversitesi'nin erişim kontrol prosedürü, kampüs alanlarında bulunan fiziksel kaynaklar, bilgi teknolojileri sistemleri ve diğer kritik varlıkların güvenliğini sağlamak amacıyla oluşturulmuştur.

2. KAPSAM

Bu prosedür, üniversitenin kaynaklarını, sistemlerini ve diğer kritik bilgilerini korumak için gerekli olan tüm erişim noktalarını kapsamaktadır.

3. UYGULAMA

3.1. FİZİKSEL ERİŞİM KONTROLÜ

3.1.1. Kritik tüm sistemler ve sunucular mutlaka fiziksel olarak korumalı sistem odalarında muhafaza edilir.

3.1.2. Sistem odaları kapıları mutlaka kapalı tutulur ve erişimler mutlaka yetkilendirilmiş çalışanlar tarafından kimlik doğrulama (RFID kimlik kartı) sistemleri ile yapılır.

3.1.3.Erişim kontrol mekanizmasına ait günlük kayıtlar (log) saklanır ve değiştirilmeye karşı korunur.

3.1.4. Sistem odalarına giriş yetkisi olmayan ancak bakım / onarım, danışmanlık vb. gibi amaçlarla sistem odasında çalışma ihtiyacı olan kişilere, içeride bulunduğu süre boyunca, yetkili bir personel refakat eder.

3.1.5. "Çok Gizli ve Gizli" gizlilik derecesine sahip bilgiler, kilitli dolaplarda muhafaza edilir, aksi durumda yetkili personel ilgili odayı terk ederken kapının kilitlendiğinden emin olur.

3.2. SİSTEM ERİŞİMİ KONTROLÜ

3.2.1. İşletim sistemlerine erişim tek faktörlü kimlik doğrulama ile sağlanır. İşletim sistemlerinde kullanıcılara verilecek erişimlerin detayları bu Prosedürün Kullanıcı Erişim Yönetimi Bölümü'nde belirtilmiştir. İşletim sistemi erişimleri domain için belirlenmiş kullanıcı adı ve parolası ile gerçekleştirilir. Kullanıcı doğrulamasını domain kontrolü gerçekleştirir. Parolaların korunması ve yönetimi ile ilgili Parola Prosedüründe belirtilen hususlar işletim sistemlerine erişim için de geçerlidir.

3.2.2. Sistem yöneticileri kendilerine ait yönetici hesaplarına sahiptir.

3.2.3. Kullanıcılar kimlik doğrulaması yaparak oturum açtıkları sistemlerin başından ayrıldıklarında sistemi kilitlerler.

3.2.4. Sistem erişimlerinde yetkisiz erişimlerin kısıtlanması için mutlaka şifre kontrolü yapılır.

3.2.5. Şifresiz erişilebilen sunucu bulunmaz.

3.2.6. Sistemlere erişimlerde ortak hesap kullanılmaz.

3.2.7. Erişim yetkileri verilirken "bilmesi gerektiği kadar prensibi" ne göre hareket edilir.

3.2.8. Sistemlere uzaktan erişim gerektiren durumlarda "Uzaktan Çalışma Prosedürü dokümanında yer alan yazılı kurallara uyulur.

3.2.9. Son kullanıcıların kullandığı ağ ile sistemlerin bulunduğu genel ağ birbirinden ayrılır.

3.3. AĞ ERİŞİM KONTROLÜ

3.3.1. Kritik Sistemlerin bulunduğu ağ diğer ağlardan ayrılır ve erişimi kısıtlanır.

3.3.2. Ağ cihazlarının bulunduğu ağ diğer ağlardan ayrılır ve erişimi kısıtlanır.

3.3.3. Uzaktan erişimler için sadece yetki verilen sistemin bulunduğu ağa ve cihaza erişecek şekilde yetkilendirme yapılır.

3.3.4. Kablosuz ağlarda "Varsayılan SSID (Service Set Identifier)" isimleri kullanılmaz.

3.4. KABLOSUZ AĞ CİHAZLARINA ERİŞİM KONTROLÜ

3.4.1. Tüm bu ağların yönetimi BT tarafından gerçekleştirilir. Ağlar için yapılacak tüm yapılandırma ve uygulanacak tüm kontroller BT tarafından gerçekleştirilir.

3.4.2. Kullanıcılar, bilgisayar ağını ve ağ servislerini diğer kullanıcıların ağ ve ağ servislerini kullanımını engelleyecek veya ağ servislerine ve bileşenlerine zarar verecek şekilde kullanamaz.

3.4.3. Kullanıcılar, bilgisayar ağını ve ağ servislerini kullanarak spam, zararlı kod, yazılım vb. unsurları gönderemez, başka kullanıcıların bilgisayarlarına saldırmak için kullanamaz.

3.4.4. Bilgisayar ağına, yetkisiz kişiler tarafından modem, kablosuz erişim noktası, anahtarlama cihazı veya HUB gibi cihazlar bağlanamaz.

3.4.5. Kablosuz misafir ağı ayrılmış olarak kullanılmaktadır. Misafir ağına dahil olanların logları 5651 sayılı kanuna göre 2 yıl tutulmaktadır.

3.4.6. Kurumsal kablosuz ağlar sadece kullanıcı ağı olarak yapılandırılmıştır. Kablosuz ağ üzerinden izin verilmediği taktirde diğer bilgi işleme olanaklarına erişim yapılmamaktadır.

3.4.7. Kablosuz ağ cihazlarının şifreleri BT tarafından yönetilir.

3.5. AĞ HİZMETLERİNE ERİŞİM KONTROLÜ

3.5.1. Ağ hizmetlerine erişimlerinde mutlaka tüm erişimlerin kısıtlanması için şifre kontrolü kullanılır.

3.5.2. Şifresiz erişilebilen ağ hizmeti bulunmaz.

3.6. UYGULAMA ERİŞİM KONTROLÜ

3.6.1. Kullanıcı adı ve parola kullanımı haricinde uygulamalara erişimler mümkün değildir.

3.7. UZAKTAN ERİŞİM KONTROLÜ

3.7.1. Uzaktan erişime ilişkin uyulacak esaslar "Uzaktan Çalışma Prosedürü"de yer almakta olup, erişim kontrolüne ilişkin aşağıdaki hususlar uygulanmaktadır;

3.7.2. Veri akış güvenliği arttırılmak için uzaktan erişimlerde VPN kullanılır.

3.7.3. Uzaktan erişim ihtiyacının ortadan kalkması durumunda açılmış olan hesaplar veya portlar derhal kapatılır.

3.7.4. Kablosuz ağ erişimlerine karşı da kimlik denetimi yapılması zorunludur. WPA2 (Wi-Fi Protected Access 2) şifreleme sistemi kullanılır ve kimlik doğrulaması için güçlü şifreler oluşturulur.

3.7.5. OSTİM Teknik Üniversitesi Teknik çalışanları için uzaktan bağlantı yetkileri Aktif Dizin (AD) ile sağlanır.

3.7.6. OSTİM Teknik Üniversitesi uzaktan erişim trafiği yasal sürece uygun olarak loglanır.

3.7.7. Uzaktan çalışma donanımları ve iletişim cihazları kurum tarafından yönetilen altyapının bir parçası olduğu için kullanıcılar çağrı yönlendirme, barındırma ya da uzaktan çalışma ortamına izin verilen yerin dışında bir yere genişletmek üzere diğer teknik yolları kullanmamalıdır.

3.8. BİLGİYE ERİŞİMİN KISITLANMASI

3.8.1. Domain içerisindeki kullanıcılarının bilgi erişimleri, yetki ve çalışma alanlarına göre sınırlandırılır. Bu sınırlandırmalar aşağıdakileri kapsar;

3.8.1.1. Ortak alanda bulunan klasörleri

3.8.1.2. Uygulamalar üzerinde işlenen verileri ve dokümanları

3.8.1.3. E-posta sistemini

3.8.1.4. İnternet erişimini

3.8.1.5. Kullanıcı bilgisayarı üzerindeki kurulum hakları

3.8.2. OSTİM Teknik Üniversitesi içerisinde kullanılan uygulamalarda erişim yetkileri birim ve rol bazlı olarak tanımlanmıştır. Bu uygulamalara erişim talepleri ilgili Birim Yöneticisi ve BT Birim Yöneticisinin onayları ile belirlenir.

3.9. GÜVENLİ OTURUM AÇMA

3.9.1. Oturum açma işlemleri sırasında yetkisiz kullanıcılara yol göstermemesi amacıyla yardım mesajları yayınlanmaz.

3.9.2. Oturum açma bilgileri ancak tüm veri girişi yapıldıktan sonra doğrulanır ve hatalı bir giriş yapıldıysa hangi verinin hatalı olduğu belirtilmez.

3.9.3. Başarısız oturum açma girişimi sayısının sınırlanması ve başarısız denemelerin kaydedilmesi, özel bir yetkilendirme yapılmadıkça daha sonraki oturum açma girişimlerinin engellenmesi veya belli bir süre bloke edilmesi sağlanır.

3.9.4. Maksimum oturum açma deneme sayısı aşıldığı zaman BT Birimine haber verilir.

3.10. KULLANICI KAYDETME VE KAYIT SİLME

3.10.1. Kullanıcı isimleri isim ve soy isim şeklinde birleşik verilir. Örn; Ahmet Yılmaz için kullanıcı ismi; ahmet.yilmaz

3.10.2. İstihdam sağlanan her kullanıcı için işe giriş sürecine göre İnsan Kaynakları Birimi tarafından Bilgi Teknolojileri Birimi'ne e-posta üzerinden bilgi verilir.

3.10.3. Yazılımlar ve uygulamalar ile ilgili ek yetki talepleri Birim Yöneticileri tarafından e-posta ile Bilgi Teknolojileri Birimine iletilir.

3.10.4. Oluşturulan kullanıcı hesap bilgileri kullanıcılara BT tarafından bildirilir.

3.10.5. OSTİM Teknik Üniversitesi'nde göreve yeni başlayanlar, ayrılanlar ve birim değişiklikleri nedeniyle oluşan yeni kullanıcı/yetki oluşturma ve mevcut kullanıcı/yetki iptalleri süreçleri İnsan Kaynakları Birimi tarafından Bilgi Teknolojileri Yönetimi Birimi ile koordine edilerek tamamlanır.

3.10.6. İşten ayrılan personel, geriye dönük erişim kayıtlarının tutulması için sistem üzerinden silinmez. Parolaları rastgele oluşturulmuş bir parola ile değiştirilir. Tüm gruplardan çıkartılır. Hesap pasif hale getirilir.

3.11. KULLANICI ERİŞİMİNE İZİN VERME

3.11.1. Kullanıcılara standart kullanıcı haricinde verilen izinler AD üzerinde policy'ler ile yönetilir.

3.11.2. İlk kullanıcı tanımlama talepleri İnsan Kaynakları üzerinden Bilgi Teknolojilerine iletilir.

3.11.3. Kullanıcılara verilen yetkiler, ilgili çalışanın Birim yöneticisinin onayı alınarak ve görevlerin ayrılığı ilkesi göz önünde bulundurularak tahsis edilir.

3.11.4. Hesap aktifleştirilmeden önce kullanıcılara atanacak tüm yetkilerin düzenlenmiş olduğundan emin olunur.

3.12. AYRICALIKLI ERİŞİM HAKLARI YÖNETİMİ

3.12.1. Kullanıcılara standart kullanıcı haricinde verilen izinler Birim Yöneticileri onayı ile Bilgi Teknolojileri tarafından sağlanır.

3.12.2. Sanal sunuculara erişimler sistem yöneticisi tarafından verilir.

3.12.3.Geliştirilen yazılımlar ile ilgili erişimler, yazılımın sağladığı arayüz üzerinden belirlenir.

3.12.4. Ayrıcalıklı erişim hakları taleplerinde aşağıdaki hususların belirtilmesi gereklidir:

3.12.4.1. Hangi süreler dahilinde geçerli olacağı,

3.12.4.2**.** Görevi gereği ilkesi kapsamında, hangi nedenden dolayı istendiği

3.12.4.3. İhtiyacı kadar ilkesi kapsamında, ihtiyacın sınırlarının çizilmesi,

3.12.4.4. Ayrıcalıklı erişim haklarının iz kayıtları öncelikli incelenir.

3.12.4.5. Veri tabanı ayrıcalıklı erişimleri, veri tabanı yönetimsel arayüzü tarafından sağlanır.

3.13. KULLANICILARA AİT GİZLİ KİMLİK DOĞRULAMA BİLGİLERİNİN YÖNETİMİ

3.13.1. Kullanıcılara farkındalık eğitimleri ve Bilgi Güvenliği Politikaları ile gizli kimlik bilgilerini muhafaza etmesi gerektiğine dair bilgilendirme yapılır.

3.13.2. Kullanıcıların ilk oturumlarında parolalarını değiştirmesi zorunludur.

3.13.3. Her kullanıcı için geçici parola oluşturulur.

3.13.4. Kurulum sırasında oluşan varsayılan kimlik bilgileri değiştirilerek kullanılır.

3.14. ERİŞİM HAKLARININ GÖZDEN GEÇİRİLMESİ, DÜZENLENMESİ VEYA KALDIRILMASI

3.14.1. OSTİM Teknik Üniversitesinde göreve yeni başlayanlar, işten ayrılanlar ve birim değişiklikleri BT Müdürlüğü'ne bildirilmesinden sonra en kısa sürede erişim yetkileri oluşturulur, silinir veya güncellenir.

3.14.2. Çalışmaya devam eden personele ilişkin tüm kullanıcı yetkileri BT Birim Yöneticisinin onayı ile en az yılda bir kez olmak üzere periyodik olarak gözden geçirilir.

3.14.3. Sistem ve uygulamalarda kullanıcılara verilen haklar kayıt altında tutulur. Birim Yöneticisinin yazılı onayı olmadan kimseye ek erişim hakkı verilmez.

3.14.4. OSTİM Teknik Üniversitesi'nde iş ilişkisi sonlanan kullanıcıların,

3.14.4.1. Domain hesapları iptal edilir ve ayrı bir "AYRILANLAR OU (Organisation Unit)" altında saklanır,

3.14.4.2. E-posta verileri yedeklenir, e-posta hesabı kapatılır.

3.14.4.3. E-posta yetkileri sıfırlanır, gerekli durumlarda Birim Yöneticisinin onayı ile ilgili personele yönlendirilir.

3.14.4.4. Domain Users haricindeki tüm gruplardan çıkarılır. Bağlı olduğu yönetici kaldırılır. Hesap disable edilir.

3.15. ÜÇÜNCÜ TARAF ERİŞİM KONTROLÜ

Bilgi Sistemleri ağındaki ilgili sunuculara bağlanmak için;

3.15.1. Firmalar dış bağlantılar için Gizlilik sözleşmesi imzalamalıdır.

3.15.2. Bağlantı istenen Uygulama/Sunucuna, sorumlusu ve BT Müdürü tarafından verilen onaya istinaden, BT Destek ekibi tarafından erişim yetkilendirmesi yapılır.

3.15.3. Firma çalışanı adı ve Firma bilgileri girilerek Lokal ssl vpn kullanıcı adı ve şifre tanımlanır.

3.15.4. Erişmesi gereken sunucu/lar ve portları istenip belirlenen zaman aralığında erişim verilir.

3.15.5. Firmaların uzak bağlantıları, mesai saatleri içerisinde olacak şekilde günlük olarak verilmektedir. Daha uzun süren bağlantılar için termin süresi verilerek ve mesai dışı olup olmadığını belirterek talep edilmelidir.

3.15.6. Tedarikçi firma, erişim hakkı verilen sunucuları, ticari reklamlar ve haber duyuruları gibi istenmeyen mesajları (spam) göndermek, internet servis kalitesini bozacak, karışıklık yaratacak amaçlar için kullanamaz.

3.15.7. Tedarikçi firma, erişim hakkı verilen sunucuları, kullanım amacına uygun olmayan, müstehcen, rahatsız edici materyalin üretilmesi ve dağıtılması için kullanamaz. Güvenli olmadığı bilinen sitelere (mp3, program, oyun, sohbet vb.) girmek için kullanamaz.

3.15.8. Tedarikçi firma, erişim hakkı verilen sunucuları, İftira ve karalama mahiyetindeki materyalin üretimi ve dağıtımı için kullanamaz.

3.15.9. Tedarikçi firma, erişim hakkı verilen sunucuları, başkalarının verilerini tahrip için kullanamaz.

3.15.10. Tedarikçi firma, erişim hakkı verilen sunucuları, başkalarına ait kişisel veri bilgileri tecavüz edilmesi amaçlı kullanamaz.

3.15.11. Tedarikçi firma, erişim hakkı verilen sunucuları, başkalarına ait çalışmaları bozmak, tahrip etmek için kullanamaz.

3.15.12. Tedarikçi firma, erişim hakkı verilen sunucuları, internet ağ üzerinde başkalarına kullanım olanağı vermeyecek oranda trafik yaratamaz.

3.15.13. Tedarikçi firma, erişim hakkı verilen sunucuları, başka bir kullanıcının adı ile posta sunusu üzerinden mail gönderemez.

3.15.14. Tedarikçi firma, erişim hakkı verilen sunucuları, erişim izni verilen adresleri dışındaki kurum ip adreslerine erişim isteği gönderemez.

3.15.15. Dışardan hizmet alınan üçüncü kişi kullanıcı tanımları ve buna ilişkin sorumluluklar, tedarikçilerle yapılan sözleşmeler üzerinde belirtilir.

3.15.16. Üçüncü tarafların tüm erişimleri kayıt altına alınır ve yılda bir defa gözden geçirilir.

3.15.17. Alınan hizmetin tamamlanması ile firmaların kullanıcı hesapları kapatılır.

4. REVİZYON GEÇMİŞİ

Revizyon No	Tarih	Açıklama
01	07.11.2024	Entegre Kalite Yönetim Sisteminde kalite yönetiminde zorluklar ile karşılaşılması sebebiyle ISO 9001 Kalite Yönetim Sistemi (KYS) ve ISO 27001 Bilgi Güvenliği Yönetim Sisteminin (BGYS) ve dokümanlarının ayrılması ve ayrı ayrı takip edilmeleri kabul edilmiştir. Bu sebeple doküman kodlamalarında revizyon yapılmıştır.

Hazırlayan	Kontrol Eden	Onaylayan
İlknur ALŞAHİN Kalite Birimi	Kenan IŞIK Kalite Koordinatörü	Prof.Dr. Murat Ali YÜLEK Rektör
E-imzalıdır/paraflıdır	E-imzalıdır	E-imzalıdır