1. AMAÇ

Bu politikanın amacı, Kuruluşun fiziksel alanlarına, teçhizatlarına, kuruluş bilgisayarlarında kullanılan yazılımlara ve önemli kayıtlarına yetkisiz erişimi engelleyerek Kuruluş bilgi varlıklarını korumaya ve yönetmeye yardımcı olmasıdır.

2. KAPSAM

Bu politika; bütün KURULUŞ paydaşları, Bilgi İşlem altyapısını kullanmakta olan tüm birimleri ve çalışanları kapsar.

3. SORUMLULUK

Bu politikanın kullanıcıları kuruluşun tüm çalışanlarıdır.

4. UYGULAMA

4.1. Genel Erişim kontrol Prensipleri

Erişim kontrolü, en basit tanımıyla, belli bir varlığa sadece yetkili kişi veya grupların tanımlanan haklar dahilinde erişebilmesidir. Bu erişim fiziksel olabileceği gibi mantıksal bir erişim de olabilir. En genel haliyle mantıksal erişim, bir bilgi varlığına bilgisayar aracılığıyla yapılan erişimleri ifade eder.

Bilgi güvenliği kapsamında ise erişim kontrolü kimlik doğrulama (*authentication*), yetkilendirme (*authorization*) ve izlenebilirlik (*accountability*) kavramlarını içine almaktadır. Erişim kontrol modelinde varlıklara erişenler ve sistemde aktif halde olanlara özne (*subject*), erişilen kaynaklara ise nesne (*object*) denilir. Bir erişim kontrol sisteminin sağladığı temel servisler şunlardır:

- Kimlik doğrulama ile sisteme hangi öznelerin giriş yapabileceğinin belirlenmesi.
- Yetkilendirme ile öznelerin hangi işlemleri yapmaya veya hangi nesnelere erişmeye yetkili olduğunun belirlenmesi,
- İzlenebilirlik ile öznelerin sistemde hangi işlemleri yaptıklarının veya hangi nesnelere eriştiklerinin bilinmesi ve gözlenebilmesi.

Bilinen 2 tür erişim kontrol tekniği mevcuttur. Bunlar:

- İsteğe bağlı erişim kontrol (Discretionary Access Control)
- Zorunlu erişim kontrol (Mandatory Access Control)

İsteğe bağlı erişim, kontrolde varlığa kimlerin veya hangi öznelerin, hangi yetkiler dahilinde erişebileceğini o varlığın sahibi belirler.
Zorunlu erişim kontrol tekniğinde ise erişim yetkileri varlığın (bilginin) sahibi tarafından değil sistem tarafından tanımlanır. Zorunlu erişim kontrolünde, nesnelerin içerdiği bilginin etiketle belirtilen hassasiyet derecesine ve erişimde bulunacak öznelerin sahip olduğu resmi yetkilendirmeye bağlı olarak erişim kısıtlanır.

Erişim kontrolü konusunda bilinmesi gereken önemli bir prensip bulunmaktadır. "En düşük erişim hakkı", veya diğer bir tabirle "Mümkün olan en az yetki" prensibince erişimde bulunan özneye kendisine atanmış olan görevlerini gerçekleştirmelerine yetecek en düşük seviyede erişim hakkı verilmelidir. Örneğin veri tabanından raporlama amacıyla okuma yapan bir programa sadece gerekli tablolardan okuma yapmasına izin verilmelidir. Bu programın başka tablolardan okuma yapabilmesi veya yazma işlemi gerçekleştirmesi en düşük erişim hakkı ilkesine aykırıdır. Bu prensip ayrıca kabul edilmesi gereken güvenlik ilkesi olarak da bilinir. Erişim politikası kurumun bilgi varlıklarına hangi kurallar ve şartlar dâhilinde, kimlerin (hangi öznelerin), hangi yetki ve imtiyazlarla erişebileceğini kurallar dâhilinde belirleyen dokümandır.

Fiziksel güvenlik kapsamında erişim kontrolü bir mülke, binaya veya odaya girişin sadece yetkili kişilere kısıtlanması olarak karşılık bulmaktadır. Fiziksel erişim kontrolü bir insan (güvenlik görevlisi, kapıcı vb.), mekanik engeller (kilit, anahtar vb.) veya teknolojik geçiş kontrol sistemleri (kart, parmak izi vb.) kullanılarak sağlanabilir.

4.2. Erişim Kontrol Politikasının İlkeleri

- Kullanıcıların internet ve e-posta erişimlerinin sağlanmasından Bilgi İşlem Daire Başkanlığı Network Birimi sorumludur. Kuruluş üst yönetimin onayını alarak istediği erişim haklarını kısıtlama yetkisine sahiptir.
- Üniversite çalışanları ile ilgili başvurular, Personel Yönetimi Prosedürü 'ne göre işe alındıktan sonra, internet sistemine erişim hakkı ve e-posta alt yapısı Bilgi İşlem Daire Başkanlığı tarafından sağlanmaktadır. Her bir birimin ve görev tanımının sistem üzerinden hangi yazılımlara erişeceği tanımlanır.
- Öğrencilerin kaydı yapıldıktan sonra yine Bilgi İşlem Daire Başkanlığı tarafından alt yapısı sağlanır, kullanıcı adı ve şifresi belirlenir. Öğrencilerin internet ve sisteme girişleri ile ilgili erişim yetkisi Bilgi İşlem Daire Başkanlığı tarafından verilir.

- Talepler sistem üzerinden gelmekte ve Bilgi İşlem Daire Başkanlığı tarafından onaylanmaktadır.
- Kullanıcılar SDU 'nün bilgi işlem altyapısını kullanabileceği gibi kendi özel bilgi işlem araçlarını da kullanabilirler. Kullanıcılar bilgi işlem araçlarının amaçlarına uygun olarak kullanımının denetlenmesinden sorumludurlar.
- Kullanıcıların erişim yetkisi olmayan yazılım ve sistemlere girmemeleri için gerekli altyapı Bilgi İşlem Daire Başkanlığı tarafından sağlanır.
- Bilgi İşlem Daire Başkanlığı tarafından ilgili yazılımlar vasıtası ile işten ayrılan personel ve mezun olan / ilişiği kesilen öğrencinin veya personelin kullanıcısı kapatılır. Bu işlem "İlişik Kesme Formu " kapsamında yapılır.
- Geçici süre için herhangi bir alan veya sisteme erişim sağlanacaksa bu kişi Erişim Yetkileri Listesi'ne eklenir ve süre sonunda erişim yetkileri geri alınarak liste tekrar revize edilir.
- Fiziksel erişim kısıtlamaları Erişim Yetkileri Listesi'nde belirtilmiştir. Tüm çalışanlar bu sınırlar dahilinde hareket etmelidir. Yetkisiz erişim yapılması halinde disiplin süreci başlatılır.

Erişim ile ilgili kriterler aşağıda verilmiştir.

4.3. Network Erişimi

Kurum Network altyapısında kullanılan router, switch, hub, modem vb. network yönetim cihazlarına erişim, Kurum Bilgi İşlem çalışanları tarafından belirlenen güçlü şifrelerle, yetkisiz erişimlere karşı güvenlik altına alınmıştır. Bilgi İşlem Daire Başkanlığı tarafından personel arası erişimler tanımlanmış kimin hangi alana erişebileceği belirlenmiştir. Bu kapsamda sadece Bilgi İşlem Daire Başkanlığı'nda belirlenen personelin ulaşabildiği yetki kontrollü bir alanda saklanmakta ve veri kaybına karşı bu alanın da yedeklemesi yapılmaktadır. Yönlendirici giriş portlarına gelen geçersiz IP adresleri yasaklanmıştır. Bilgisayar ağında bulunan sunucu, yazıcı, tarayıcı, switch, router, modem, firewall gibi cihazlar sabit IP adresine sahip olup cihaz IP listesinde yer almaktadır. Bunun dışında kalan tüm PC, notebook ve mobil cihazlar dinamik IP adresine sahiptir. Firmware güncellemeleri ve yapılandırma değişiklikleri önce test ortamında denendikten sonra herhangi bir sorun ile karşılaşılmaz ise mesai saatleri dışında gerçek ortama alınmaktadır. Ağ cihazlarına sadece içeriden ve güvenli ağ protokolü ile bağlanılması mümkündür.

4.4. Veri Tabanı Erişimi

Veri Tabanı Yönetimi Yazılım Birimi tarafından yapılmaktadır. Bu kişinin kullanıcı adı ve şifresi güvenli bir şekilde korunmaktadır. Bu çalışma aşağıdaki çalışmaları kapsar.

Veri Arşivleme / Kapasite Planlama: Verinin boyutunu ve büyümesini takip ederek, gerekli durumlarda arşivleme yapılır. Arşivleme işlemi yapılırken veri bütünlüğünün bozulmamasına dikkat edilir.

Kontrol: Şüpheli bir durum olduğunda SQL üzerindeki tablolara ait LOG kayıtları üzerinden yapılan işlemin ne olduğu, kimin tarafından hangi saatte yapıldığı gibi bilgileri araştırarak, konunun gerçek nedeninin bulunmasına ilişkin kayıtları tespit eder.

Uygulama Entegrasyonu: Belirli formata uygun bir veriyi dışa aktarmak (export) gerekli ise, buna ilişkin TSQL veya SSIS kodları ile isteğin yerine getirilmesini sağlar.

Yedekleme & Recovery: Kurumun verilerini korumak amacı ile periyodik yedeklemenin yapılmasını sağlar. Backup planına uygun olarak alınan yedekler, Test SQL sunucusuna ayda bir kez Restore edilir. Bu hem test veri tabanının güncellenmesini sağlar, hem de alınan yedeğin sağlıklı bir şekilde kurulup kurulamadığını gösterir.

Business Intelligence/Data Warehousing: Bu amaçla kullanılan raporlama sunucusunda gerekli geliştirmeleri yapar. Raporlama sunucusunun çalışırlığını kontrol eder.

Kurulum, Konfigürasyon, Patch Geçişi ve SQL Server Yükseltme: Patch geçme ve SQL Server sürüm yükseltme işlemleri karmaşık ve riskli operasyonlardır. Bu işlerin iyi planlanıp ve test edildikten sonra üretim ortamına alınması gerekir. Operasyona başlamadan önce gerçek ortamın tam yedeklemesi yapılır. Ardından test sunucusu üzerine Patch geçilir. Bir süre takip edildikten sonra, Cluster içindeki gerçek ortam sunuculardan önce birine patch geçilir. Yine bir sorun görülmezse diğer sunuculara da patch geçilerek kesintisiz ve güvenli bir çalışma sağlanmış olur.

Test Ortamlarını Yönetme: Gerçek ortam veri tabanı yönetiminin yanı sıra test ortamındaki veri tabanının da yönetimini gerçekleştirir.

Gizlilik: SQL Server kullanıcı girişlerinin oluşturulması, bu kullanıcı girişlerinin başka sunuculara taşınması ve bunların yönetiminden sorumludur.

4.5. İnternet Erişimi

İnternet, bilginin geniş bir alana ve hızla yayılmasına imkan verir. Bununla birlikte, SDU 'ye özgü kritik bilgilerin çalınması da mümkündür. Hassas konularla ilgilenen ve bunlara ait bilgileri internete aktaran herkes, bir bilgi güvenliği ihlalinde bulunduğunu bilmelidir.

Üniversite çalışanları, öğretim üyeleri, öğrenciler, danışmanlar, destek hizmeti veren kişi ve kurumlar, görev tanımları ve sözleşmelerde yer alan görevlerini yerine getirebilmek için

- Çalışmalarına destek olacak şekilde kendilerine sağlanacak üniversite kaynaklarını kullanarak internete erişebilirler.
- Bunun için gerekli altyapı sağlanmış, erişim için gerekli uygun donanım ve yazılım ürünlerini kurarak, kullanıcıların internet erişimlerini sağlanmaktadır.
- Bilgi İşlem Daire başkanlığı, gerekli durumlarda üniversite bünyesindeki birimlerde kurulu olan sistemlerin hızlandırılması vb. gerekli nedenlerle internet trafiği üzerinde kısıtlamalara gider ve kullanıcıların kullanım kapasitelerini düşürebilir.

4.5.1. İnternet Kullanırkan Dikkat Edilmesi Gereken Kurallar

Üniversite'de internet kullanım hakkı genel olarak iş amaçlı verilmektedir. Bununla birlikte çalışanlar/öğrenciler konuya sadece medya kullanım bilinci ve sorumluluğu ile yaklaştıkları sürece, ayrıca kurumsal uyum yasaları çerçevesinde diğer erişimleri de desteklenir.

Bu konudaki en önemli noktalar üniversitenin kendi uzmanlık alanıyla ilgili kritik bilgilerinin, gizlilik kurallarının ve üniversite imajının korunmasıdır. Oluşabilecek potansiyel tehlikeler kurum iletişim ağını kullanan çalışanların/öğrencilerin bazı basit kurallara uyması durumunda en aza inecektir.

- Hiçbir kullanıcı dosya paylaşım siteleri ve peer to peer bağlantı yolu ile internetteki servisleri kullanamaz.
- Her türlü sohbet programının kullanıcılar tarafından bilgisayarlarda kurulması, kullanılması veya internet siteleri üzerinden kullanılması kesinlikle yasaktır. Ancak iş tanımına göre belirli kullanıcılara işin gerektirdiği ihtiyaç doğrultusunda Bilgi İşlem Daire Başkanlığı onayıyla izin verilebilir.
- Üniversite çalışanları/öğrenciler, BGYS ile yürürlükteki Türkiye Cumhuriyeti yasaları ve yönetmeliklerine uygun hareket etmeli ve kesinlikle interneti aykırı faaliyetlerde bulunmak için kullanmamalıdır.
- Bilgisayar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.

- Sistemi gereksiz meşgul edecek, çalışmalar için kullanılmayan ve internet trafiğini gereksiz yere artıracak, müzik ve resim dosyaları, oyunlar, filmler ve benzeri programların (zip, rar, mpg, mpeg, avi, exe, com, mp3 vb. uzantılı dosyalar) internetten indirilmesi yasaktır.
- İnternet üzerinden Bilgi İşlem Daire Başkanlığı tarafından onaylanmamış yazılımlar indirilemez ve üniversite altyapısı üzerine bu yazılımlar kurulamaz. Bu konuda kendi inisiyatifinizle yaptığınız her şey ciddi sonuçlara yol açabilir. Kurumsal işlevlere yönelik yazılım ihtiyaçlarının olması durumunda bilgi işlem daire başkanlığına bildirim yapılmalıdır.
- İnternete üniversitenin/kişisel taşınabilir bilgisayar ile bağlanılıyorsa en güncel virüs tarayıcı bilgisayara yüklenir ve çalıştığı kontrol edilir. Üniversite iletişim ağını Internet risklerine karşı koruyabileceğimiz tek yol budur. Bunun dışındaki Internet üzerindeki diğer tüm servisler gereksiz güvenlik riskleri içermektedir.
- Üçüncü şahısların kurum internetini kullanmaları Bilgi İşlem Daire Başkanlığı izni ve bu konudaki kurallar dahilinde gerçekleştirilir. İnternete aynı ağ ile bağlanmaz.
- İnternet erişiminin tüm günlükleri (Log Kayıtları) arşivlenir. Bu kayıtlar üniversite ve her bir kullanıcı bazında kaydedilir. Üniversitenin teknik bilgi birikimi ve ticari çıkarları, her zaman için korunmalıdır.
- Üniversite çalışanları, görev tanımları ve sözleşmelerde tanımlı görevlerini yerine getirilebilmek için çalışmalarına destek olacak şekilde İnternet aracılığı ile dağıtılan bazı ücretsiz sürüm programlarını kullanmak istemeleri halinde Bilgi İşlem Daire Başkanlığı'na başvurmaları gerekmektedir. Bu tür programların internet üzerinden indirilmesi, kurulması sadece Bilgi İşlem Daire Başkanlığı personeli tarafından yapılır.
- Üniversiteye ait her türlü bilgi, doküman ve/veya yazılımın, iş amaçlı kullanım dışında, İnternet üzerinden satılması veya kurum dışındaki üçüncü kişilere herhangi bir sebeple gönderilmesi kesinlikle yasaktır.
- Üniversite içi kullanımı için hazırlanmış herhangi bir bilgi, dosya veya duyurunun (iş potansiyelleri, birim maliyetleri, fiyatlar, yatırımlar, ihale bilgileri vb.) İnternet üzerinden açıklanması veya dağıtılması Rektörlük inisiyatifindedir.
- Üniversiteye ait önemli bilgilerin yetkisiz kişilere verildiği veya açıklandığı tespit edildiğinde veya bu konuda şüphe oluştuğunda Bilgi İşlem Daire Başkanlığı ile zaman geçirilmeden paylaşılmalıdır.