T.C.

İSTANBUL MEDİPOL ÜNİVERSİTESİ

BİLGİ TEKNOLOJİLERİ DAİRESİ

BİLGİ GÜVENLİĞİ POLİTİKALARI

KILAVUZU*

İSTANBUL

2016

İÇİNDEKİLER

ÖNSÖZ

İstanbul Medipol Üniversitesi verdiği eğitim ve kattığı farklılıklarla, kalıcı üstünlükler kazanmış, bilim ve teknoloji üretimine odaklı, toplumun değişen ihtiyaçlarına cevap verebilen bireyler yetiştirmeyi ilke edinmekte, topluma ve evrensel bilime katkıda bulunmayı görev kabul etmektedir. Bu misyonla yoluna hızlı adımlarla devam eden üniversitemizde Bilgi Teknolojileri en üst seviyede kullanılmaktadır. Bu kapsamda, özellikle personel ve öğrencilerimize ait kişisel bilgiler ile tüm resmi yazışmalar tamamen elektronik ortamlarda bulunmakta ve işlenmektedir. Bu durum, kişisel bilgilerin sahiplerinin isteği dışında, ilgisiz ve yetkisiz kişi veya kişilerin eline geçmesi, kişisel bilgilerin sahiplerine zarar verebilecek boyutta yasa dışı olarak kullanılması ve kişi mahremiyetinin ihlali tehlikesini de beraberinde getirmektedir. Dolayısıyla her geçen gün gelişen bilgi teknolojileri, bilgi güvenliği olgusunu da bir zorunluluk haline getirmiştir.

Bu ihtiyaçtan yola çıkarak Üniversitemiz bünyesinde bulunan kişisel ve tüzel bilgilerin gizlilik, bütünlük ve erişilebilirlik ilkeleri çerçevesinde önlemlerin alınması, risklerin belirlenerek indirgenmesi amacıyla bilgi güvenliğine ilişkin kuralların yazılı olarak belirlendiği Bilgi Güvenliği Politikası oluşturulmuştur. Bu politikadan İstanbul Medipol Üniversitesi kapsamında bulunan her türlü bilgiyi üreten, işleyen, bu bilgilere doğrudan veya dolaylı olarak erişen herkes sorumludur.

1. BİLGİ GÜVENLİĞİ

Günümüzde devlet kurumları ve ticari şirketler işlerini sürdürebilmek için yoğun bir şekilde bilgi kullanımına yönelmişlerdir. Zaman geçtikçe bilginin önemi artmış, sadece güvenli bir şekilde saklanması ve depolanması gelişen ihtiyaçlara cevap verememiş aynı zamanda bir yerden bir yere nakil edilmesi de kaçınılmaz bir ihtiyaç haline gelmiştir. Bilgiye olan bu bağımlılık bilginin korunması ihtiyacını gündeme getirmiştir. Bu anlamda bilgi, kurumun sahip olduğu varlıklar arasında çok önemli bir yere sahiptir. Bilgiye yönelik olası saldırılar, tahrip edilmesi, silinmesi, bütünlüğünün ve/veya gizliliğinin zarar görmesi, bilgi altyapısının bozulmasına ve bu da beraberinde işlerin aksamasına neden olmaktadır. Bu çerçevede bilgi ve bilgi güvenliği kavramları karşımıza çıkmaktadır.

Bilgi güvenliği, "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak" tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı ise "kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır.

Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlıktır. Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar.

Bilgi birçok biçimde bulunabilir. Bilgi, kâğıt üzerinde yazılı olabilir, elektronik olarak saklanıyor olabilir, posta ya da elektronik posta yoluyla bir yerden bir yere iletilebilir ya da kişiler arasında sözlü olarak ifade edilebilir. Bilgi hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır. Bilgi güvenliğinin sağlanabilmesi bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin yeterli düzeylerde sağlanabilmesi ile mümkündür.

Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:

Şekil 1- Gizlilik, Bütünlük, Süreklilik BİLGİ G ÜVENLİĞİ

• Gizlilik

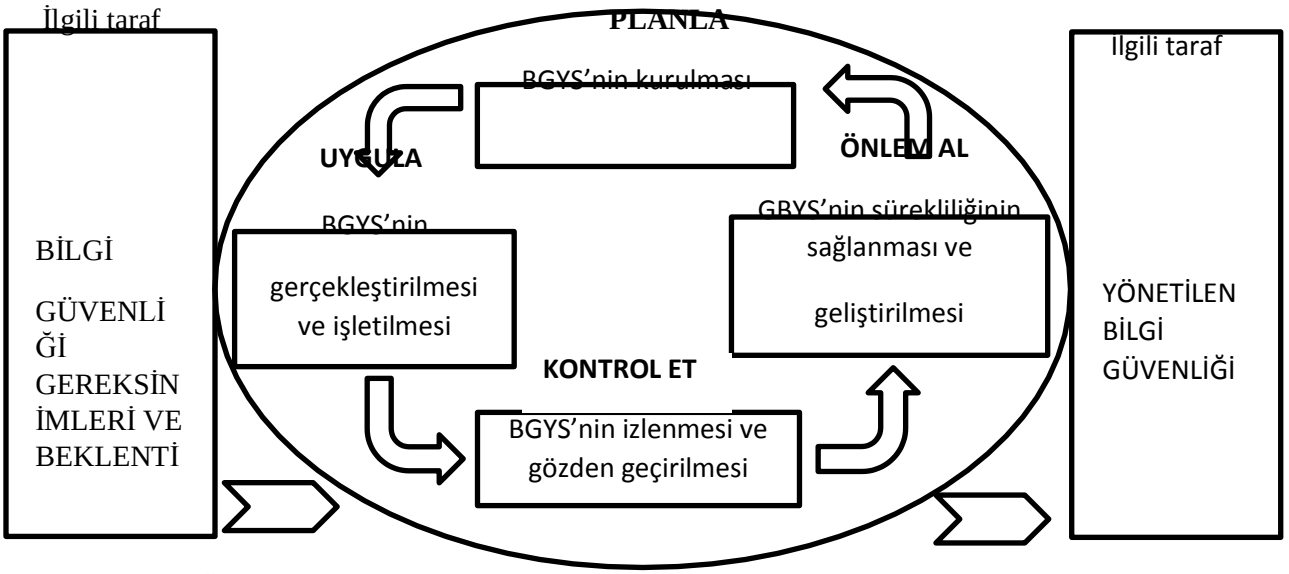
• Bütünlük

• Süreklilik

Bu kavramları biraz daha açacak olursak gizlilik, bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir. Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz. Kullanılabilirlik, bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

2. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Bilgi Güvenliği Yönetim Sistemi BGYS, kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. Bu sistemin temel amacı hassas bilginin korunmasıdır. Bu sistem çalışanları, iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini kapsar. BGYS standartları kapsamında BGYS'in kurulumu, gerçeklenmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve tekrar gözden geçirilmesi için PUKÖ (Planla – Uygula – Kontrol et – Önlem al) modeli kullanılmaktadır. . PUKÖ modelini görsel olarak anlatan Şekil 2, bir BGYS'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve prosesler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını nasıl ürettiğini gösterir.



Şekil 2- PUKÖ Modeli

2.1. RİSK YÖNETİMİ

Risk Yönetimi bir kurumun ya da kuruluşun çalışabilirliği, ticari kuruluşlar içinse öncelikle kârlılığını olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir. Risk yönetiminde, riskin tamamıyla ortadan kaldırılması mümkün değildir. Sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla

gereksiz kayıpların engellenmesi amaçlanmaktadır. Başarılı bir risk yönetimi için, kuruluşların bilgi varlıklarına ve hedeflerine yönelik risklerin belirlenerek, analiz edilmesi, tanımlanan risklerin denetim altında tutularak izlenmesi gereklidir. Riski yönetmenin en doğru yolu, gerçekleşme olasılığı ve gerçekleştiğinde vereceği zarar en yüksek olan riskleri azaltacak bilgi teknolojisi risk yönetim sürecinin oluşturulmasıdır.

2.1.1. Varlıkların Belirlenmesi

Varlık, sistemin bir parçası olan ve kurum için değeri olan her şeydir. Varlık kurum için değer taşıdığından korunması gerekir. Bir BT sisteminde sadece yazılım ve donanımlar varlık olarak düşünülmemelidir. Aşağıdaki örnekler varlık olarak nitelendirilebilecek değerlerdir.

a. Bilgi,
b. Donanım (kişisel bilgisayarlar, yazıcılar, sunucular),
c. yazılım (işletim sistemleri, geliştirilen uygulamalar, ofis programları),
d. haberleşme cihazları (telefonlar, hatlar, kablolar, modemler, anahtarlama cihazları),
e. dokümanlar(stratejik toplantıların tutanakları, sözleşmeler vb.),
f. üretilen mallar,
g. servisler,
h. personel,
i. kurumun prestiji / imajı.

2.1.2. Tehditlerin Belirlenmesi

Tehdit, herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir. Tehdit kaynağı ise varlıklara zarar verme olasılığı olan olaylar ve durumlar olarak tanımlanabilir. En bilinen tehdit kaynakları şunlardır: Doğal tehditler: Deprem, sel, toprak kayması, yıldırım düşmesi, fırtına gibi tehditler. Çevresel tehditler: Uzun süreli elektrik kesintileri, hava kirliliği, sızıntılar vs. İnsan kaynaklı Tehditler: İnsanlar tarafından yapılan veya yol açılan bilinçli veya bilinçsiz olaylar. Örneğin yanlış veri girişi, ağ saldırıları, zararlı yazılımların yüklenmesi, yetkisiz erişimler vs.

Aşağıdaki tablo BT sistemlerinde sıklıkla karşılaşılan tehditleri ve bunların kaynaklarını içermektedir (tehdidin kaynağı bölümünde kullanılan kısaltmalar B: İnsan kaynaklı ve bilerek, K: İnsan kaynaklı ve kazayla, D: Doğal, Ç:Çevresel).

Tehdit	Tehdidin Kaynağı
Deprem	D
Sel	D
Fırtına	D
Yıldırım	D
Endüstriyel bilgi sızması	B,K
Bombalama ve silahlı saldırı	B
Deprem	D
Güç kesintisi	B,K,Ç
Su kesintisi	B,K,Ç
Havalandırma sisteminin arızalanması	B,K,Ç
Donanım arızaları	K
Güç dalgalanmaları	K,Ç
Tozlanma	Ç
Elektrostatik boşalma	Ç
Hırsızlık	B
Saklama ortamlarının izinsiz kullanılması	B,K
Saklama ortamlarının eskiyip kullanılmaz	K

duruma gelmesi	
Personel hataları	K
Bakım hataları/eksiklikleri	K
Yazılımların yetkisiz kullanılması	B,K
Kullanıcı kimlik bilgilerinin çalınması	B,K
Zararlı yazılımlar	B,K
Yetkisiz kişilerin ağa erişimi	B
Ağ cihazlarının arızalanması	K
Hat kapasitelerinin yetersiz kalması	B,K
Ağ trafiğinin dinlenmesi	B
İletim hatlarının hasar görmesi	B,K
Mesajların yanlış yönlendirilmesi	K
Mesajların yetkisiz kişilere yönlendirilmesi	B
İnkar etme	B
Kaynakların yanlış kullanımı	K
Kullanıcı hataları	K
Personel yetersizliği	K

2.1.3. Açıklıkların Belirlenmesi

Açıklık, sistem güvenlik prosedürlerinde, tasarımda, uygulamada veya iç kontrollerde bulunan ve bilgi güvenliği ihlal olayına sebep olabilecek zayıflık, hata veya kusurlardır. Açıklıklar tek başlarına tehlike oluşturmazlar ve gerçekleşmeleri için bir tehdidin mevcut olması gerekir. Açıklık değerlendirmesi, tehditler tarafından gerçekleştirilebilecek açıklıkları ve bu açıklıkların ne kadar kolay gerçekleştirilebileceğini ele alır. Açıklıkların belirlenmesinde anket, birebir görüşme, dokümantasyon ve otomatik tarama araçları gibi yöntemler kullanılabilir.

2.1.4. Olasılık Değerlendirmesi

Risk analizinde bir açıklığın gerçekleşme olasılığının belirlenmesi büyük önem taşır ve tespit edilen tüm açıklıklar için olasılık değerlendirmesi yapılmalıdır. Olasılığın belirlenmesi için tehdit kaynağının motivasyonu ve becerisi, açıklığın cinsi, mevcut kontrollerin varlığı ve etkinliği göz önünde bulundurulmalıdır.

Olasılık değerlendirmesi için kurum kaç kademeli bir değerlendirme yapacağını ve kademelerin nasıl belirleneceğini tanımlamalıdır. Üç seviyeli bir olasılık değerlendirmesi için aşağıdaki örnek tablo kullanılabilir.

OLASILIK SEVİYESİ	OLASILIK SEVİYESİ
Yüksek	Tehdit kaynağı çok kabiliyetli ve motivasyonu yüksektir, açıklığın gerçekleşmesini engelleyecek kontroller bulunmamaktadır veya etkisizdir.
Orta	Tehdit kaynağı kabiliyetli ve motivasyonu yüksektir, açıklığın gerçekleşmesine engel olacak kontroller mevcuttur.
Düşük	Tehdit kaynağı daha az kabiliyetli ve motivasyonu daha düşüktür, açıklığın gerçekleşmesini engelleyecek veya çok zorlaştıracak kontroller mevcuttur.

2.1.5. Etki Analizi

Risk derecelendirmesi yapabilmek için olasılık değerlendirmesinden sonra gelen adım etki analizidir. Etki analizinde herhangi bir açıklığın gerçekleşmesi halinde yaşanacak olası olumsuz etki seviyesi belirlenir. Bunun için varlığın görevi, kritikliği, varlığın etkilediği verinin hassasiyeti ve varlığın

mali değeri göz önüne alınmalıdır. Bu bilgiler daha önceden yapılmış iş etki analizi raporlarından alınabilir. Eğer daha önce yapılmış böyle bir çalışma yoksa sistemin kritiklik seviyesi sistemin (ve sakladığı veya işlediği verinin) bütünlüğünü, gizliliğini ve erişilebilirliğini korumak için gerekli koruma göz önüne alınarak niceliksel olarak çıkarılabilir. Ayrıca sistemin yenilenme maliyeti, çalışmaması durumunda oluşabilecek gelir kaybı gibi bazı niteliksel etkiler de etki analizinde göz önüne alınabilir. Niceliksel bir etki analizinde olasılık değerlendirmesinde olduğu gibi kurum kaç kademeli bir değerlendirme yapacağını ve kademelerin nasıl belirleneceğini tanımlamalıdır.

Etki Derecesi	Etki tanımı
YÜKSEK	Açıklığın gerçekleşmesi durumunda: Kurumun en önemli varlıkları çok fazla etkilenir veya kaybedilir ve mali zarar çok büyük olur. Kurumun çıkarları, misyonu ve prestiji büyük zarar görebilir veya etkilenebilir. İnsan hayatı kaybı veya ciddi yaralanmalar gerçekleşebilir.
ORTA	Açıklığın gerçekleşmesi durumunda: Kurumun önemli varlıkları etkilenir ve kurum mali zarara uğrar. Kurumun çıkarları, misyonu ve prestiji zarar görebilir veya etkilenebilir. Yaralanmalar gerçekleşebilir.
DÜŞÜK	Açıklığın gerçekleşmesi durumunda: Kurumun bazı varlıkları etkilenir Kurumun çıkarları, misyonu ve prestiji etkilenebilir.

2.1.6. Risk Derecelendirmesi

Bu adımın amacı, varlıkları tehdit eden risklere değerler atayıp onları derecelendirmektir. Uygun kontrollerin seçilmesi burada belirlenen risklere ve seviyelere göre yapılır. Risk bir tehdidin bir açıklığı gerçekleme olasılığının, açıklığın ne kadar kolay gerçekleştirilebildiğinin ve mevcut veya planlanan kontrollerin yeterliliğinin bir fonksiyonudur. Yani kısaca olasılık değerlendirmesinde ve etki analizinde belirlenen değerlere bağlıdır. Risklerin ölçülebilmesi için risk sınıflandırma matrisi oluşturulmalıdır ve bu sınıflandırma için tanımlamalar yapılmalıdır.

2.1.7. Risk Derecelendirme Matrisi

Yukarıda örnek olarak verilen üç seviyeli olasılık değerlendirmesi ve etki analizi için şu şekilde bir risk derecelendirme matrisi oluşturulabilir.

Etki Seviyesi				
Düşük	Orta	Yüksek		
Düşük	Düşük	Düşük	Düşük	Olma Olasılığı
Düşük	Orta	Orta	Orta	
Düşük	Orta	Yüksek	Yüksek	

Bu matristeki değerleri kurum kendisi belirlemelidir. Bunun için istenirse sayısal değerler kullanılabilir. Örneğin olma olasılıklarına 0 ile 1 arasında, etki seviyesine ise 0 ile 100 arasında değerler atanır. Risk dereceleri için aralıklar belirlenir. Olma olasılığı ve etki seviyesi çarpımının düştüğü aralık risk derecesini belirler. Örneğin bu matrise göre olma olasılığı "Orta" ve etki seviyesi "Yüksek" olan bir açıklığın risk derecesi "Orta" olarak sınıflandırılmıştır.

2.1.8. Risk Derecelerinin Tanımı

Risk derecelendirme matrisinde belirlenen risk dereceleri bir açıklığın gerçekleşmesi halinde karşı karşıya olunan riski belirlemektedir. Bu risk derecelerinin tanımlanması yönetimin risklerle ilgili alacağı kararlar açısından önemlidir. Ayrıca bu aşamada kurumun kabul edebileceği risk seviyesi de belirlenmelidir. Belirlenen bu seviyeye göre kurum bazı riskleri kabul ederek karşı önlem almamayı tercih edebilir. Yukarıdaki risk seviye matrisine uygun olarak aşağıdaki tanımlamalar örnek olarak gösterilebilir.

Risk Derecesi	Risk Açıklaması ve yapılması gerekenler
Yüksek	Düzeltici önlemlerin alınması şarttır. Mevcut sistem çalışmaya devam edebilir ama hangi önlemlerin alınacağı ve nasıl uygulanacağı olabildiğince çabuk belirlenmelidir ve önlemler uygulanmalıdır.
Orta	Düzeltici önlemlerin alınması gerekmektedir. Hangi önlemlerin alınacağı ve nasıl uygulanacağına dair plan makul bir süre içerisinde hazırlanmalı ve uygulanmaya başlanmalıdır.
Düşük	Önlem alınıp alınmayacağı sistem sahibi/sorumlusu tarafından belirlenmelidir. Eğer yeni önlemler alınmayacaksa risk kabul edilmelidir.

2.1.9. Uygun Kontrollerin Belirlenmesi

Yapılan risk derecelendirme çalışmalarının sonucunda risklerin azaltılmasını veya ortadan kaldırılmasını sağlayacak kontrol önerileri belirlenmelidir. Önerilecek kontrollerin amacı riski kurumun kabul edebileceği bir değere düşürmek olmalıdır. Önerilecek kontrollerde kontrollerin etkinliği, yasalar ve düzenlemeler, iş yapma biçimine getireceği değişiklikler, kurum politikaları ve güvenlik konuları dikkate alınması gereken başlıca konulardır. Uygulanabilecek olası kontroller belirlenirken başvurabilecek kaynaklardan biri "TS ISO/IEC 27001:2005 Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardıdır. Bu standart, güvenlik politikası, bilgi güvenliği organizasyonu, varlık yönetimi, insan kaynakları güvenliği, fiziksel ve çevresel güvenlik, haberleşme ve işletim yönetimi, erişim kontrolü, bilgi sistemleri edinim, geliştirme ve bakımı, bilgi güvenliği ihlal olayı yönetimi, iş sürekliliği yönetimi ve uyum ana başlıkları altında pek çok kontrol önerisi içermektedir. Ayrıca bu kontrollerin gerçekleştirilmesine ait öneriler ve en iyi uygulamalar için TS ISO/IEC 27002:2005 standardına başvurulmalıdır.

3. POLİTİKALAR

3.1. EPOSTA POLİTİKASI

3.1.1. E-Posta ile ilgili yasaklanmış kullanım kuralları aşağıda belirtilmiştir.

a. Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.
b. Üniversite ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.
c. Kullanıcı, Üniversitenin e-posta sistemini taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında ilgili birime haber verilmelidir.
d. ç) Kullanıcı hesapları, ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçlar ile e-posta gönderilmemelidir.
e. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, ilgili birime haber verilmelidir.
f. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
g. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.
h. Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların yollanmasından sorumludur.

3.1.2. E-Posta ile ilgili kişisel kullanım kuralları aşağıda belirtilmiştir.

a. E-posta kişisel amaçlar için kullanılmamalıdır.
b. Kullanıcı, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidir. Bu yüzden parola kullanılmalı ve kullanılan parola en geç 45 günde bir değiştirilmelidir. E-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
c. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e- postalara herhangi bir işlem yapmaksızın ilgili birime haber vermelidir.
d. ç) Kullanıcı, kurumsal mesajlarını, kurum iş akışının aksamaması için cevaplandırmalıdır.
e. Kullanıcı, kurumsal e-postalarının, kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesini ve okunmasını engellemelidir.
f. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar ilgili birime haber verilmelidir.
g. 6 ay süreyle kullanılmamış e-posta adresleri kullanıcıya haber vermeden sunucu güvenliği ve veri depolama alanının boşaltılması için kapatılmalıdır.
h. Kullanıcı parolaları, en az 8 karakterden oluşmalı ve parolalarının içinde; en az 1 tane harf, en az 2 tane rakam ve en az 1 tane özel karakter (@,a,+,$,#,&,/,{,*,- ,],=...)içermelidir.
i. ğ) Kullanıcı, kendilerine ait e-posta parolasının güvenliğinden ve gönderilen e- postalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren ilgili birime haber vermelidir.
j. Kurumsal e-postalar yetkili kişilerce hukuksal açıdan gerekli görülen yerlerde önceden haber vermeksizin denetlenebilir.
k. Kullanıcı, e-postalarına erişirken, POP3, SMTP, HTTP vb kullanıcı adı ve parolasını açık metin olarak (okunabilir halde) taşıyan protokolleri kullanmamalıdır.

l. Kurum, e-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur.
m. Virüs, solucan, truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslere bulaşmış e-postalar antivirüs yazılımları tarafından analiz edilip, içeriği korunarak virüslerden temizlenmelidir. Ağa dâhil edilmiş bilgisayarlarda ve sunucularda ağ güvenlik yöneticileri bu yazılımdan sorumludur.

3.2. PAROLA POLİTİKASI

3.2.1. Parola Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

a. Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) en geç 6(altı) ayda bir değiştirilmelidir.
b. Kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) en geç 45(kırk beş) günde bir değiştirilmelidir.
c. Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır. ç) Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
d. Kullanıcı, parolasını başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda bilgilendirilmeli ve eğitilmelidir.
e. Kurum çalışanı olmayan kişiler için açılan kullanıcı hesapları da kolayca kırılamayacak güçlü bir parolaya sahip olmalıdır.
f. Bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.

3.2.2. Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır.

a. En az 6 haneli olmalıdır.
b. İçerisinde en az 1 tane harf bulunmalıdır. (a, b, C...)
c. İçerisinde en az 2 tane rakam bulunmalıdır. (1, 2, 3...)
d. ç) İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,a,+,$,#,&,/,{,*,-,],=,...)
e. Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, ababab...)
f. Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,1234,zxcvb...)
g. Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)

3.2.3. Şifre koruma standartları ile ilgili kurallar aşağıda belirtilmiştir.

a. Bütün parolalar Kuruma ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.
b. Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki “parola hatırlama” seçeneği kullanılmamalıdır.
c. Parola kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir.
d. ç) Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilebilir.

3.2.4. Uygulama Geliştirme Standartları

a. Bireylerin ve grupların kimlik doğrulaması işlemini desteklemelidir.
b. Parolalar metin olarak veya kolay anlaşılabilir formda saklanmamalıdır.
c. Parolalar, şifrelenmiş olarak saklanmalıdır.
d. ç) En az RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

3.3. ANTİVİRUS POLİTİKASI

3.3.1. Antivirus Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Kurumun tüm istemcileri ve sunucuları antivirüs yazılımına sahip olmalıdır. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak antivirüs yazılımı yüklenmeyebilir.
b. İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalıdır.
c. Sistem yöneticileri, antivirüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
d. Kullanıcı hiç bir sebepten dolayı antivirüs yazılımını bilgisayarından kaldırmamalıdır.
e. Antivirüs güncellemeleri antivirüs sunucusu ile yapılmalıdır. Sunucular internete sürekli bağlı olup, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, otomatik olarak antivirüs sunucusu tarafından antivirüs güncellemeleri yapılmalıdır.
f. Etki alanına dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarları ağdan çıkartabilmelidir.
g. Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.
h. Kurumun ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.
i. Optik Media ve harici veri depolama cihazları antivirüs kontrolünden geçirilmelidir.
j. Kritik veriler ve sistem yapılandırmaları düzenli aralıklar ile yedeklenmeli ve bu yedekler farklı bir elektronik ortamda güvenli bir şekilde saklanmalıdır. Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı olmalıdır.

3.4. İNTERNET ERİŞİM VE KULLANIM POLİTİKASI

3.4.1. İnternet Erişim ve Kullanım Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar(lar)ı üzerinden internete çıkmalıdır. Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.
b. Kurumun politikaları doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografi, oyun, kumar, şiddet içeren vs.) yasaklanmalıdır.
c. Kurumun ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır.
d. Kurumun ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılmalıdır. İnternete giden ve gelen bütün trafik virüslere karşı taranmalıdır.
e. Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri hayata geçirilmelidir.
f. Ancak yetkilendirilmiş kişiler internete çıkarken, Kurumun normal kullanıcılarının bulunduğu ağdan farklı bir ağda olmak kaydıyla, bütün servisleri kullanma hakkına sahiptir.
g. Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemelidir.
h. İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilmemeli ve indirilmemelidir. Bu konuda gerekli önlemler alınmalıdır.
i. Üçüncü şahısların internet erişimleri için misafir ağı erişimi verilmelidir.

3.5. SUNUCU GÜVENLİK POLİTİKASI

3.5.1. Sahip olma ve sorumluluklar ile ilgili kurallar aşağıda belirtilmiştir.

a. Kurum'da bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel(ler) sorumludur.
b. Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel(ler) tarafından yapılmalıdır.
c. Sunuculara ait bilgilerin yer aldığı tablo oluşturulmalıdır. Bu tabloda, sunucuların isimleri, ip adresleri ve yeri, ana görevi ve üzerinde çalışan uygulamalar, işletim sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personel(ler)in isimleri ve telefon numaraları bilgileri yer almalı ve bu tablo bir portal üzerinde bulundurulmalıdır.
d. Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.

3.5.2. Genel yapılandırma kuralları aşağıda belirtilmiştir.

a. Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri Kurum'un Başkanlık Sistem Şubesi Biriminin talimatlarına göre yapılmalıdır.
b. Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
c. Servislere erişimler, kaydedilerek ve erişim kontrol yöntemleri ile koruma sağlanmalıdır.
d. Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve antivirüs vb. koruma amaçlı yazılımlar sürekli güncellenmelidir. Antivirüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılmalıdır. Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, bir onay ve test mekanizmasından geçirilmeli, sonra uygulanmalıdır. Bu çalışmalar için yetkilendirilmiş bir personel olmalıdır.
e. Sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.
f. Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
g. Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.
h. Sunucular üzerinde lisanslı yazılımlar kurulmalıdır.
i. Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

3.5.3. Sunucu gözlemleme kuralları aşağıda belirtilmiştir.

a. Kritik sistemlerde, uygulamalar kaydedilmeli ve kayıtlar aşağıdaki gibi saklanmalıdır.
b. Kayıtlara çevrimiçi olarak minimum 90 gün süreyle erişebilmelidir.
c. Günlük tape backuplar en az 1 ay saklanmalıdır.
d. Haftalık tape backuplar en az bir ay saklanmalıdır.
e. Aylık full backuplar en az 6 (altı) ay saklanmalıdır.
f. Kayıtlar sunucu üzerinde tutulmalarının yanı sıra ayrı bir sunucuda da saklanmalıdır.
g. Sunucu üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları, vb.) çalıştırılmamalıdır.
h. Kayıtlar sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.
i. Port tarama atakları düzenli olarak yapılmalıdır.
j. Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik yapılmalıdır.
k. Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.
l. Denetimler, Bilgi İşlem grubu tarafından yetkilendirilmiş kişilerce yönetilmeli ve belli aralıklarda yapılmalıdır.
m. Sunucuların bilgileri yetkilendirilmiş kişi tarafından Tablo (Ek-2)'deki bilgileri kapsayacak şekilde tutulmalı ve güncellenmelidir.

3.5.4. Sunucu işletim kuralları aşağıda belirtilmiştir.

a. Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, tavan ve taban güçlendirmeleri yapılmış ortamlarda bulundurulmalıdır.
b. Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.
c. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve bilgisayar sistemine kayıt edilmelidir.

3.6. AĞ CİHAZLARI GÜVENLİK POLİTİKASI

3.6.1. Ağ cihazları güvenlik politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Ağ cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer almalıdır.
b. Yerel kullanıcı hesapları açılmamalıdır. Ağ cihazları kimlik tanımlama için LDAP, RADIUS veya TACAS+ protokollerinden birini kullanmalıdır.
c. Yönlendirici ve anahtarlardaki tam yetkili şifre olan ‘enable şifresi’ kodlanmış formda saklanmalıdır. Bu şifrenin tanımlanması kurumun içerisinden yapılmalıdır.
d. Kurumun standart olan SNMP community string’leri kullanılmalıdır. Bu bilgi sadece yetkilendirilmiş kişiler tarafından bilinmelidir.
e. İhtiyaç duyulduğu zaman erişim listeleri eklenmelidir.
f. Yönlendirici ve anahtarlar kurumun yönetim sisteminde olmalıdır.
g. Yazılım ve firmware güncellemeleri önce test ortamlarında denenmeli, sonra çalışma günlerinin dışında üretim ortamına taşınmalıdır.
h. Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.
i. Bilgisayar ağında bulunan kabinetler, aktif cihazlar, ağ kabloları (UTP ve fiber optik aktarma kabloları), cihazların portları etiketlenmelidir.
j. Her bir yönlendirici ve anahtar aşağıdaki uyarı yazısına sahip olmalıdır. Yönlendiriciye erişen tüm kullanıcıları uyarmalıdır.

“BU CİHAZA YETKİSİZ ERİŞİMLER YASAKLANMIŞTIR. Bu cihaza erişim ve yapılandırma için yasal hakkınız olmak zorundadır. Bu cihaz üzerinde işletilen her komut loglanabilir, bu politikaya uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptırım olabilir.”

3.7. AĞ YÖNETİM POLİTİKASI

a. Ağ cihazları yönetim sorumluluğu, sunucu ve istemcilerin yönetiminden ayrılmalıdır.
b. Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılmalı ve güncellemeler uygulanmalıdır.
c. Erişimine izin verilen ağlar, ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmeli ve yetkisiz erişimle ilgili tedbirler alınmalıdır.
d. Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanmalıdır.
e. Sınırsız ağ dolaşımı engellenmelidir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaçlara göre serbest bırakılmalıdır.
f. Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınmalıdır.
g. İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmalı ve kayıtlar tutulmalıdır.

h. Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır. Kurum kullanıcılarının bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılmalı ve ağlar arasında geçiş güvenlik sunucuları (firewall) üzerinden sağlanmalıdır.
i. Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.
j. Bilgisayar ağına bağlı bütün makinelerde kurulum ve yapılandırma parametreleri, Kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.
k. Sistem tasarımı ve geliştirilmesi yapılırken Kurum tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanılmalıdır.
l. İnternet trafiği, İnternet Erişim ve Kullanım Politikası ve ilgili standartlarda anlatıldığı şekilde izlenebilmelidir.
m. Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı şekilde saklanmalıdır.
n. Ağ cihazları görevler dışında başka bir amaç için kullanılmamalıdır.
o. Ağ cihazları yapılandırılması Sistem Yöneticisi tarafından veya Sistem Yöneticisinin denetiminde yapılmalı ve değiştirilmelidir.
p. Ağ dokümantasyonu hazırlanmalı ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanmalıdır.

3.8. UZAKTAN ERİŞİM POLİTİKASI

a. Internet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamaktadır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. Protokollerinden birini içermelidir.
b. Uzaktan erişim güvenliği denetlenmelidir.
c. Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.
d. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.
e. Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılmalıdır.
f. Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve antivirüs yazılımı güncellemeler yapılmış olmalıdır.
g. Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

3.9. ERİŞİM YÖNETİMİ VE ERİŞİM KAYITLARININ TUTULMASI POLİTİKASI

Veri tabanlarına erişen kullanıcıların yapmış oldukları işlemler loglanmalı, gerektiğinde erişim yetkilisinin kayıt silme logları da listelenebilir olmalıdır.

3.9.1. Erişim Yönetimi

Kurumun erişim sağlanacak sunucularına admin/root yetkili yönetici kullanıcılar, sudo ve runas yetkili kısıtlı yönetici kullanıcılar ve dış dünyadan erişen, uygulamayı kullanan kullanıcılardan oluşmaktadır.

a) Bakanlık sunucularına erişim için IP/SEC ya da SSL VPN kullanılmalıdır. Mümkünse kullanıcıların erişimi için SSL ve VPN tercih edilmelidir. Güvenlik Birimi tarafından sağlanmalıdır.
b) Sunuculara kullanıcı erişimi için SSH, RDP gibi protokollerle sunucu yönetimi için belirli portlar erişim verilmelidir.
c) Sunucuların kendi aralarında servis ve yönetimleri için belirli portlarla erişim sağlanması gerekmektedir.
d) Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir. Parola yönetimi bakanlık bilgi güvenliği kılavuzundaki parola yönetim politikaları ile yürütülmelidir.
e) Kullanıcıların sunucu yönetim için sağlanan erişimde merkezi kullanıcı yönetimi (MS AD, LDAP, ssh-key) ile yapılmalıdır.
f) Kullanıcıların sunucu yönetim için sağlanan erişimde sudo, runas gibi erişim kısıtlı erişim yetkileri tanımlanmalıdır.
g) Dış dünyadan sunucular üzerindeki servislere erişim için 80, 443, 7001, 8080, 8443 gibi servis portları da özel durumlarda verilmelidir. Güvenlik Birimi tarafından bu işlem sağlanmalıdır.
h) Sunucu servislerinin yönetim işlemlerinde yetkili kullanıcı bilgileri, sistem gurubuna teslim edilmelidir. Sistem birimi nezaretinde ve tarafından yürütülmelidir.
i) Sunucu servislerinin yönetim işlemleri merkezi kullanıcı yönetimi ve kısıtlı erişim yetkileriyle kullanıcılara sağlanmalıdır.
j) Kurumun yedekleme sistemlerine sadece memur ya da danışman yetkili kişi erişim yapmaktadır. Firmaların yapacakları tüm işlemler sistem birimi nezaretinde yürütülmelidir.

3.9.2. Kayıt Tutulması (Log tutulması)

a) Kurumun güvenlik cihazlarına ait loglar güvenlik birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.
b) Kurumun veri tabanlarına ait loglar veri tabanları birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır
c) Kurumun network cihazlarına ait loglar network birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır
d) Tüm sunuculara ve servislere sağlanan tüm yönetici erişimleri uzak ve merkezi bir kayıt sunucusuna gönderilmelidir.
e) Merkezi kayıt sunucusu üzerinde yapılan analizler sonucunda başarısız erişimler raporlanmalıdır.
f) Merkezi kayıt sunucusu üzerinde alınan başarısız erişim istekleri uyarı olarak yetkili Birimlere gönderilmelidir.
g) Merkezi kayıt sunucusu üzerindeki başarılı girişler de istatiksel veriler halinde raporlanabilmelidir.

h) Merkezi kayıt sunucusu üzerindeki kayıt verileri belirli tarih aralığında tutulmalı ve istenildiğinde raporlanabilir olmalıdır.
i) Merkezi kayıt sunucusu kayıtlar üzerinde yaptığı analizler doğrultusunda saldırı ve normal olmayan durumları tespit edip, uyarı gönderebilmelidir.

3.9.3. Uzaktan Erişim Yönetimi

a) Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.
b) İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamalıdır. VPN teknolojileri İpSec, SSL, VPDN, PPTP, L2TP vs. protokollerinden birini içermelidir.
c) Uzaktan erişim güvenliği sıkı şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one-time password authentication, örnek; Token Device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmelidir. Daha fazlası için parola politikasına bakınız.
d) Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.
e) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.
f) Mobile VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile yapılmalıdır.
g) Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.
h) Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.
i) Uzak erişimde yapılan tüm network hareketleri loglanmalıdır.
j) Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.
k) Uzak erişim verilecek olan kullanıcılara sözleşmesine göre günlük saatlik izinler verilmelidir. Sınırsız izin verilmekten kaçınılmalıdır.
l) VPN ile erişecek olan kullanıcı VPN Erişim formunu doldurmak zorundadır.
m) Uzak erişim bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmelidir.

3.9.4. Acil Erişim Yetkilendirme Yönetimi

a) Acil erişim yetkilendirme gerektiren durumlarda uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.
b) Kurum bünyesindeki bütün dahili sunucuların, ağ güvenliği ve şebeke cihazları ile veri tabanı yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur.
c) Kurum bünyesindeki yazılım ve veri güvenliğini sağlarken yetkilendirilmiş sistem yöneticisi Güvenliği sağlamaktan sorumlu Ağ ve Sistem Güvenliği birimi ile birlikte uyumlu çalışarak sağlamak zorundadır.
d) Sunuculara ve cihazlara acil erişim yetkilendirilmesi gereken durumlarda; kurum içi kullanıcı, yetkilendirilmiş sistem yöneticisine başvurarak sistem üzerinde yetki istemelidir.
e) Veri tabanına acil erişim yetkilendirilmesi gereken durumda; kurum içi kullanıcı için erişim yetkilendirmesinde veri tabanı güvenlik politikası maddelerine bakılır.
f) Acil erişim yetkisi gereken durumlarda kurum dışı kullanıcılar için resmi taahhütname gelmeden uzak erişim yetkisi verme isteği acil erişim gereken birim yetkilisi tarafından verilmelidir.

g) Başka birimlerden alınması gereken erişim yetkisinin sorumluluğu, isteği yapan birimin yetkilendirilmiş yöneticisinin sorumluluğundadır.
h) Sistem üzerinde verilecek erişim yetkisi ve bunun doğuracağı sorumluluk sunucu/cihaz üzerinde yetki veren yetkilendirilmiş sistem yöneticisinindir.
i) Kritik sistemlerde veri güvenliğini sağlamak için sistem yöneticisi gerekli güvenlik tedbirlerini almalıdır. Güvenliği sağlamak için gereken durumlarda başka birimler ile birlikte çalışmalıdır.
j) Veri tabanlarında bulunan bir veriye acil olarak erişilmesi gerektiğinde, verinin bulunduğu tablonun sahibinden eposta ortamında izin alındıktan sonra erişim izni veri tabanı birimi tarafından verilmelidir.

3.10. KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI

a) Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecek ve dokümante edilecektir.
b) Kurum sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve
c) kimlik doğrulama yöntemleri tanımlanacak ve dokümante edilecektir.
d) Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veritabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, dokümante edilmeli ve denetim altında tutulmalıdır.
e) Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve bu gereksinimler gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.
f) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.
g) Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulmalı, tekrarlanan başarısız erişim istekleri/girişimleri incelenmelidir.
h) Kullanıcılara erişim hakları yazılı olarak beyan edilmelidir.
i) Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.
j) Sistemler üzerindeki tüm roller, rollere sahip kullanıcılar ve rollerin sistem kaynakları üzerindeki yetkileri uygun araçlar kullanılarak belirli aralıklarla listelenmelidir. Bu listeler yetki seviyeleri ile karşılaştırılmalıdır. Eğer uyumsuzluk varsa dokümanlar ve yetkiler düzeltilerek uyumlu hale getirilmelidir.

3.11. KABLOSUZ İLETİŞİM POLİTİKASI

a) Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınmalıdır.

a) Bütün kablosuz erişim cihazları Bilgi İşlem Güvenlik Birimi tarafından onaylanmış olmalı ve Bilgi İşlemin belirlediği güvenlik ayarlarını kullanmalıdır.
b) Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.
c) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılmalıdır. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır.
d) Erişim cihazlarındaki firmwareler düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlamaktadır.
e) Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.
f) Varsayılan SSID isimleri kullanılmamalıdır. SSID ayarı bilgisi içerisinde kurumla ilgili bilgi olmamalıdır, mesela kurum ismi, ilgili bölüm, çalışanın ismi vb.
g) Radyo dalgalarının binanın dışına taşmamasına özen gösterilmelidir. Bunun için çift yönlü antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanmalıdır.

h) Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Kurum kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanmalı ve Kurum kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenmelidir.
i) Erişim Cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dâhil olmalıdırlar.
j) Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından Kurum'un tüm internet bant genişliğinin tüketilmesi engellenmelidir.
k) Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlı olmalıdır.
l) Kullanıcı bilgisayarlarında kişisel antivirüs ve güvenlik duvarı yazılımları yüklü olmalıdır.
m) Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

3.12. BİLGİ SİSTEMLERİ GENEL KULLANIM POLİTİKASI

a) Kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, Kurumun bünyesinde oluşturulan tüm veriler Kurumun mülkiyetindedir.
b) Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanmamalıdır. Bu konuda ilgili politikalar dikkate alınmalıdır.
c) Kurum, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
d) Kurum bilgisayarları etki alanına dahil edilmelidir. Etki alanına bağlı olmayan bilgisayarlar yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi olmamalıdır.
e) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır.
f) Kurumda Bilgi İşlem Dairesinin bilgisi ve onayı olmadan Kurum Ağ sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.
g) Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilememelidir.
h) Bilgisayarlara lisanssız program yüklenmemelidir.
i) Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
j) Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Başkanlık'a da haber verilmelidir.
k) Bütün cep telefonu ve PDA (Personal Digital Assistant) cihazları kurumun ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (kızılötesi, bluetooth, vb) özellikleri aktif halde olmamalıdır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.
l) Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve mümkünse dosyalar sıkıştırılmalıdır.

3.13. DONANIM VE YAZILIM ENVANTERİ OLUŞTURMA POLİTİKASI

a) Bu sunuculara sistem biriminin admin/root yetkisi bulunmalıdır. Yapılacak tüm işlemler sistem güvenlik birimi nezaretinde yürütülmelidir. Kuruma ait sunucularda, sadece yetkili kişilerin erişebileceği administrator/root yetkisi bulunmalıdır.
b) Kuruma ait sunucular üzerinde bulunan, tüm kullanıcı hesapları (administrator ve root hesaplarıda dahil olmak üzere) güçlü şifreler ile korunmalıdır.
c) Yapılacak tüm işlemler düzgün bir şekilde dokümante edilmeli ve ilgili birim sorumlularına iletilmelidir.

d) Güvenlik yazılım ve donanımlarının erişim logları, merkezi log sisteminde tutulmalı ve izlenmelidir.
e) Güvenlik yazılım ve donanımlarının logları, her bir yazılım ve donanım için belirlenen disk alanlarında tutulmalı ve ilgili birim tarafından yönetilmelidir.
f) Güvenlik donanımları, yetkisiz kişiler tarafından erişilememesi için gerekli güvenlik tedbirleri alınmış sistem odalarında tutulmalıdır.
g) Güvenlik donanımlarının konfigürasyon yedekleri düzenli olarak alınmalı ve bir back-up sunucusunda tutulmalıdır.
h) Kurumda kullanılan güvenlik yazılım ve donanımları en güncel ve stabil yamaya (patch) sahip olmalıdır.
i) Kurumda kullanılan güvenlik donanımları, harici izleme yazılım ya da donanımları ile izlenmeli ve cihazlarda oluşan sorunlar sms ve/veya eposta aracılığı ile ilgili sorumlulara iletilmelidir.
j) Kurumun tüm istemcileri ve sunucuları anti-virüs yazılımına sahip olmalıdır. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak anti-virüs yazılımı yüklenmeyebilir.
k) İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalıdır.
l) Sistem yöneticileri, anti-virüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
m) Kullanıcı hiç bir sebepten dolayı anti-virüs yazılımını bilgisayarından kaldırmamalıdır.
n) Anti-virüs güncellemeleri anti-virüs sunucusu ile yapılmalıdır. Sunucular internete sürekli bağlı olmalı, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, anti-virüs sunucusu tarafından anti-virüs güncellemeleri otomatik olarak yapılmalıdır.
o) Etki alanına dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarların internet bağlantılarını kesebilme opsiyonuna sahip olmalıdır.
p) Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.
q) Kurumun ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.
r) Optik Media ve harici veri depolama cihazları anti-virüs kontrolünden geçirilmelidir.

3.13.1. Yazılım Güvenliği

a) Kurum içerisinde kullanılan tüm bilgisayarların zararlı yazılımlara karşı en güncel anti virüs yazılımına sahip olmalıdır.
b) Bilgisayarlarda kullanılan anti virüs yazılımları düzenli olarak güncellenmelidir.
c) Bilgisayarların üzerinde kullanılan işletim sistemleri düzenli olarak güncelleştirilmelidir.
d) Bilgisayarlar üzerinde korsan yazılımlar bulundurulmamalıdır.
e) Kurum için hazırlanacak uygulamalar güvenlik zafiyetlerini en aza indirmek için güvenli yazılım yaşam döngüsüne uygun olarak tasarlanmalıdır.
f) Geliştirilen yazılımlar gizlilik, bütünlük ve erişebilirlik şartlarına uygun olmalıdır.
g) Yazılım geliştirme sürecinde, giriş doğrulama, yetkilendirme, kimlik doğrulama, konfigürasyon yönetimi, hassas bilgi, kriptografi, parametre manipülasyonu, hata yönetimi ve kayıt tutma ve denetimi kriterleri dikkate alınmalıdır.
h) Yazılım geliştirme süreci boyunca, gerekli bütün testler eksiksiz şekilde yapılmalıdır.
i) Kurum için geliştirilen uygulamalar ve satın alınan yazılımlar, güvenlik zafiyetlerine neden olmamak için en son stabil yamalara ve güncelleştirmelere sahip olmalıdır.

j) Uygulamalar geliştirilme süreçlerinde gerçek ortamda uygulanmadan önce test sunucularında test edilmelidir. Uygulamalar gerçek ortamda kurumun uygun bulduğu mesai saatleri dışında bir zaman diliminde devreye alınmalıdır.
k) Kurum için geliştirilen uygulamalar, uluslararası kabul görmüş standartlara bağlı dokümante edilmelidir. Uygulama için yazılmış olan dokümanlar uygulama ile beraber kuruma teslim edilmelidir.

3.13.2. Donanım Güvenliği

a) Kuruma ait sistemler ve sunucular dışarıdan gelebilecek saldırılara karşı, güncel teknolojilere sahip donanımsal firewall cihazları ile korunmalıdır.
b) Kurum çalışanlarının internete çıkışlarının kontrol edilerek, zararlı ve kurum politikasına uymayan sitelere erişimlerinin engellenmesi için proxy cihazları ile korunmalıdır.
c) Kuruma ait uygulamaların güvenli bir şekilde çalışması ve uygulamalara gelebilecek saldırıların engellenmesi için Web Application Firewall (Web Uygulama Güvenlik Duvarı) ile korunmalıdır.
d) Kurum ile dış dünya arasında ki yazışmalar bir eposta güvenlik cihazı ile kontrol edilmelidir. SPAM, virüs, kurum politikalarına uygun olmayan içerikler engellenmelidir.
e) Kurumda ki güvenlik cihazları sürekliliğin sağlanması için cluster (yedekli yapıda) bulunmalıdır.
f) Kurumda kullanılan güvenlik cihazlarının loglarının düzenli olarak alınması ve encrypt (şifreli) olarak saklanması gerekmektedir.
g) Kurumda kullanılan bütün güvenlik cihazlarının konfigürasyon yedekleri periyodik olarak alınmalı, doğru şekilde etiketlenerek saklanmalıdır.
h) Kurumda kullanılan bütün sistem ve güvenlik donanımları, kurumun ihtiyaçlarına bağlı olarak sadece izin verilen erişimlere göre konfigüre edilmelidir.

3.14. TAŞINABİLİR MATERYAL GÜVENLİĞİ POLİTİKASI

a) Oluşturulan envanter tablosunda şu bilgiler olmalıdır: sıra no, bilgisayar adı, bölüm, marka, model, seri no, özellikler, ek aksamlar, işletim sistemi, garanti süresi vs.
b) Bu tablolar merkezi bir web sunucuda tutulmalı ve belirli aralıklarla güncellenmelidir. İlgili siteye girişler güvenlik politikaları çerçevesinde yapılmalıdır.
c) Envanter bilgileri sık sık kontrol edilmelidir. Bu şekilde bilgi eksikliğinin yol açacağı kayıp ve maliyetlere engel olunmalıdır.

3.15. KRİZ/ACİL DURUM POLİTİKASI

a) Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve dokümante edilmelidir.
b) Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Problem durumlarında sistem kesintisiz veya makul kesinti süresi içerisinde felaket ve/veya iş sürekliği merkezi üzerinden çalıştırılabilmelidir.
c) Bilişim sistemlerinin kesintisiz çalışmasının sağlanması için aynı ortamda Kümeleme veya uzaktan kopyalama veya yerel kopyalama veya pasif sistem çözümleri hayata geçirilmelidir. Sistemler tasarlanırken minimum sürede iş kaybı hedeflenmelidir.
d) Acil durumlarda kurum içi işbirliği gereksinimleri tanımlanmalıdır.
e) Acil durumlarda sistem kayıtları incelenmek üzere saklanmalıdır.
f) Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma
g) oluşturulmalıdır.
h) Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
i) Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.

j) Acil durumlarda bilgi güvenliği yöneticisine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmeli ve zararın tespit edilerek süratle önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.
k) Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.

3.16. BİLGİ GÜVENLİĞİ ULAŞTIRMA GÜVENLİĞİ YÖNETİMİ

a) "Gizlilik" uygulamasının amacı, kamu kurum ve kuruluşlarının güvenliğini sağlamak, yürütülen işlemlerin ve muhafaza edilen her türlü gizlilik dereceli, bilgi, belge, evrak, doküman ve malzemelerin, düşman veya yetkili ve ilgili olmayan kimseler tarafından öğrenilmesine veya elde edilmesine engel olmaktır. Bu amaca ulaşmak için yapılan bütün düzenlemelere ve alınan bütün önlemlere" güvenlik tedbirleri" denir.
b) Taşınılabilir materyaller üzerine iletilen verinin içeriği ile ilgili herhangi bir şey yazmamalıdır. Genel başlıklar kullanmalıdır. Örneğin gizli evrakların bulunduğu bir cd üzerine "gizli evraklar" yazılmamalıdır.
c) İçinde veri bulunan taşınır materyal başka bir yere gönderiyorsa tutanak ile yetkili bir kişiye teslim edilmelidir.
d) Harici taşınabilir disklerin içi mekanik yapıya sahip olduğundan dolayı darbelere karşı çok hassastır. Bu nedenle kullanırken ve taşırken dikkat edilmelidir. Örneğin özellikle hard diskler taşınırken koruyucu kılıflar içerisinde taşınmalıdır.
e) Çok gizli evraklar, torba veya çanta gibi kilitli muhafaza içinde ve "Çok Gizli" gizlilik dereceli güvenlik belgesi olan özel kurye ile gönderilirler. Eğer normal kargo ile gönderilmesi zorunlu ise, içerik uygun bir şekilde kripto edilir (şifrelenir). Dışarıdan kargonun takip edilmemesi için kargo takip numarasının maskelenmesi yapılmalıdır.
f) Gizli evraklar veya cd, dvd, usb bellekler gönderilirken, iki adet zarf kullanmalıdır. Birinci zarfın üzerine içeriğin niteliğine göre sınıflandırılmalı ve zarfın kapağı mühürlenmelidir. İkinci zarf ise normal adres yazılan zarf olmalıdır. "GİZLİ" yazılı olan zarf diğer normal zarfın içine koyulmalıdır.

3.17. FİZİKSEL GÜVENLİK POLİTİKASI

a) Kurumun binalarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilmelidir.
b) Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binalarda ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.
c) Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili güvenlik görevlileri gözetiminde gerçekleştirilmelidir.
d) Kritik bilgilerin bulunduğu alanlara girişlerin kontrolü akıllı kartlar veya biyometrik sistemler ile yapılmalı ve izlenmelidir.
e) Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.
f) Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanmalıdır.
g) Kritik sistemler özel sistem odalarında tutulmalıdır.
h) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalı ve iklimlendirilmesi sağlanmalıdır.
i) Fotokopi, yazıcı vs. türü cihazlar mesai saatleri dışında kullanıma kapatılmalı, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınmalıdır.
j) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.

3.18. VERİTABANI GÜVENLİK POLİTİKASI

a) Veritabanı sistemleri envanteri dokümante edilmeli ve bu envanterden sorumlu personel tanımlanmalıdır.
b) Veritabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.
c) Veritabanı sistem kayıtları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.
d) Veritabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir.
e) Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.
f) Yedekleme planları dokümante edilmelidir.
g) Manyetik kartuş, DVD veya CD ortamlarında tutulan log kayıtları en az 2 (iki) yıl süre ile güvenli ortamlarda saklanmalıdır.
h) Veritabanı erişim politikaları "Kimlik Doğrulama ve Yetkilendirme" politikaları çerçevesinde oluşturulmalıdır.
i) Hatadan arındırma, bilgileri yedekten dönme kuralları "Acil Durum Yönetimi" politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.
j) Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
k) Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında
l) yetkili bir personel bilgilendirilmelidir.
m) Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.
n) Bilgi saklama medyaları kurum dışına izinsiz çıkartılmamalıdır.
o) Sistem dokümantasyonu güvenli şekilde saklanmalıdır.
p) İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.
q) Veritabanı sunucusu sadece ssh, rdp, ssl ve veritabanının orijinal yönetim yazılımına açık olmalı; bunun dışında ftp, telnet vb. gibi açık metin şifreli bağlantılara kapalı olmalıdır. Ancak ftp, telnet vb. açık metin şifreli bağlantılar veri tabanı sunucudan dışarıya yapılabilir.
r) Uygulama sunucularından veritabanına rlogin vb. şekilde erişememelidir.
s) Veritabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak kurumun kasasında saklanmalı ve gereksiz yere açılmamalıdır. Zarfın açılması durumunda firma yetkilileri de bilgilendirilmelidir.
t) Arayüzden gelen kullanıcılar bir tabloda saklanmalı, bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmalıdır.
u) Veritabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak bağlanılmalıdır. Root veya admin şifresi tanımlı kişi/kişilerde olmalıdır.
v) Bağlanacak kişilerin kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.
w) Bütün kullanıcıların yaptıkları işlemler kaydedilmelidir.
x) Veritabanı yöneticiliği yetkisi sadece bir kullanıcıda olmalıdır.
y) Veritabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.
z) Veritabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar tesis edilmelidir.
aa) Veritabanı sunucularına ancak yetkili kullanıcılar erişmelidir.
bb) Veritabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıclar bağlanıp sorgu yapmamalıdır.
cc) Veritabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir. (Ağ trafiğini dinleyen casus yazılımların verilere ulaşamaması için)

dd) Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için Şifreleme Politikasına bakılmalıdır.
ee) Veritabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için de geçerlidir.

3.19. DEĞİŞİM YÖNETİM POLİTİKASI

a) Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante
b) edilmelidir.
c) Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.
d) Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve dokümante edilmelidir.
e) Değişiklikler gerçekleştirilmeden önce Güvenlik Politikaları yöneticisi ve ilgili diğer yöneticilerin onayı alınmalıdır.
f) Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.
g) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.
h) Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmelidir.
i) Teknoloji değişikliklerinin Kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmeli ve dokümante edilmelidir.

3.20. BİLGİ KAYNAKLARI ATIK VE İMHA POLİTİKASI

a) Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.
b) Yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.
c) Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmi Gazete 'de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleşmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.
d) İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.
e) Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.
f) Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.
g) Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
h) Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.
i) Hacimsel küçültme işlemi için parçalanmalıdır.
j) Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.
k) Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

3.21. BİLGİ GÜVENLİĞİ TEKNİK VE FARKINDALIK EĞİTİMLERİ

a) Kurum içerisinde bilgi güvenliği teknik ve farkındalık eğitimleri için yıllık bir plan yapılmalıdır.
b) Yıllık planlar çerçevesinde bilgi güvenliği teknik ve farkındalık eğitimleri gerçekleştirilmelidir.
c) Sunulan bilgi güvenliği teknik ve farkındalık eğitimleri katılım öncesi ve sonrası çeşitli ölçme teknikleriyle ölçülmeli ve eğitim etkililiği hususunda değerlendirme yapılmalıdır.
d) Kurumların teknik işlerinde (Bilişim faaliyetleri), uygulama geliştirme, sistem güvenliği kapsamında hizmet veren personellerin kişisel gelişimlerinin devamlılığı konusunda eğitimler düzenlenmelidir.
e) Eğitime katılım formları muhafaza edilmelidir.
f) Eğitim faaliyetleri işlemlerinin, kurum içerisinde nasıl yürütülmesi gerektiği hususunda bir prosedür geliştirilmelidir.

3.22. VERİ YEDEKLEME VE İŞ SÜREKLİLİĞİ POLİTİKASI

a) Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerini ve kurumsal veriler düzenli olarak yedeklenmelidir.
b) Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde ve offline olarak manyetik kartuş, DVD veya CD ortamında yedekleri alınmalıdır.
c) Taşınabilir ortamlar (manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından faklı odalarda veya binalarda güvenli bir şekilde saklanmalıdır. Veriler offline ortamlarda en az 2 (iki) yıl süreyle saklanmalıdır.
d) Kurumsal kritik verilerin saklandığı veya sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.

e) Düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamaların çalıştığı ve yedeği alınacak dizin, dosya bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.
f) Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
g) Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.
h) Yedek ünite üzerinde gereksiz yer tutmamak amacıyla, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dâhil edilmemelidir.
i) Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.
j) Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenmelidir.
k) Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.
l) Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
m) Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dâhilinde tamamlanması gerekmektedir.
n) Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.
o) Yedekleme Standardı ile doğru ve eksiksiz yedek kayıt kopyaları bir felaket anında etkilenmeyecek bir ortamda bulundurulmalıdır.
p) Veri Yedekleme Standardı, yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği belirlenmelidir. Yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerliği periyodik olarak gözden geçirilmelidir.

3.23. SON KULLANICI GÜVENLİĞİ POLİTİKASI

a) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.
b) Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilmeli ve teyit alınmalıdır.
c) Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorulması sağlanmalıdır.
d) Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.
e) Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.
f) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.
g) İş tanımı değişen veya Kurumdan ayrılan kullanıcıların erişim hakları kaldırılmalıdır.
h) Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
i) Kurum bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı, eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.
j) Yetkiler, "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı", rollerin ve sorumlulukların paylaştırılması ile ilgilidir. Bu paylaşım ile kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılmalıdır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla yetkiyle donatılmamasıdır. Sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmalıdır.

k) Çalışanlar, kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler, görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe alınan elemanlar için de bu eğitim, uyum süreci sırasında verilmelidir.
l) Çalışanların güvenlik ile ilgili aktiviteleri izlenmelidir.
m) Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır.

3.24. BAKIM POLİTİKASI

a) Kurum sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için gerekli anlaşmalar için yıllık bütçe ayrılmalıdır.
b) Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.
c) Sistem üzerinde yapılacak değişiklikler ile ilgili olarak "Değişim Yönetimi Politikası" ve ilişkili standartlar uygulanmalıdır.
d) Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenmelidir.
e) Sistem bakımlarının ilgili politika ve standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik uygunluk ve güvenlik testleri yapılmalıdır.
f) Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda "İstanbul Medipol Üniversitesi Bilgi Güvenlik Politikaları" uyarınca hareket edilmelidir.

3.25. YAZILIM GELİŞTİRME POLİTİKASI

a) Sistem yazılımında mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.
b) Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.
c) İhtiyaçlar, uygun bir şekilde tanımlanmalıdır.
d) Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.
e) Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.
f) Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.
g) Hazırlanan sistemler mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları belgelenerek onaylanmalıdır.
h) Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.
i) Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.
j) Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.
k) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.
l) Yazılımlar sınıflandırılmalı / etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

3.26. MAL VE HİZMET ALIMLARI POLİTİKASI

a) Mal ve hizmet alımlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilmelidir.
b) Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır:

3.27. BİLGİ GÜVENLİĞİ POLİTİKASI

a) Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,
b) Gerekli fiziki koruma için kontrol ve mekanizmalar,
c) Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,
d) Varlıklarda oluşan herhangi bir değişimin tespiti için prosedürler; örneğin, bilgi, yazılım ve donanımda oluşan kayıp veya modifikasyon,
e) Anlaşma sırasında, sonrasında ya da zaman içinde kabul edilen bir noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,
f) Varlıklarla ilgili gizlilik, bütünlük, elverişlilik ve başka özellikleri,
g) Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,
h) Kullanıcı ve yönetici eğitimlerinin methodu, prosedürü ve güvenliği,
i) Bilgi güvenliği sorumluluğu ve sorunları için kullanıcı bilinci sağlama,
j) Uygun olduğu yerde personel transferi için hüküm,
k) Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar,
l) Açık bir raporlama yapısı ve anlaşılan raporlama formatı,
m) Değişim yönetimi sürecinin açıkça belirlenmesi,
n) Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları,
o) İzin verilen erişim yöntemleri, kullanıcı kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,
p) Kullanıcı erişimi ve ayrıcalıkları için bir yetkilendirme süreci,
q) Korumanın bir gerekliliği olarak mevcut hizmetleri kullanmaya yetkili kişilerin ve hakları ile ayrıcalıkları gibi kullanımları ile ilgili olan bir bilgilerin bir listesi,
r) Erişim haklarının iptal edilmesi veya sistemler arası bağlantı kesilmesi için süreç,
s) Sözleşme de belirtilen şartların ihlali olarak meydana gelen bilgi güvenliği ihlal olaylarının ve güvenlik ihlallerinin raporlanması, bildirimi ve incelenmesi için bir anlaşma,
t) Sağlanacak ürün veya hizmetin bir açıklaması ve güvenlik sınıflandırması ile kullanılabilir hale getirilmesini tanımlayan bir bilgi,
u) Hedef hizmet seviyesi ve kabul edilemez hizmet seviyesi,
v) Doğrulanabilir performans kriterlerinin tanımı, kriterlerin izlenmesi ve raporlanması,
w) Kuruluşun varlıkları ile ilgili herhangi bir faaliyetin izlenmesi ve geri alınması hakkı,
x) Üçüncü bir taraf tarafından yürütülen denetimler için sözleşmede belirtilen denetleme sorumlulukları hakkı ve denetçilerin yasal haklarının sıralanması,
y) Sorun çözümü için bir yükseltme sürecinin kurulması,
z) Bir kuruluşun iş öncelikleri ile uygun elverişlilik ve güvenilirlik de dahil olmak üzere hizmet sürekliliği gerekleri,

3.27.1. Anlaşmayla ilgili tarafların yükümlülükleri,

a) Hukuki konularla ilgili sorumlulukları ve yasal gereklerin nasıl karşılanması gerektiğinden emin olunmalıdır, (örneğin, veri koruma mevzuatı, anlaşma diğer ülkelerle ile işbirliği içeriyorsa özellikle farklı ulusal yargı sistemleri dikkate alınarak)
b) Fikri mülkiyet hakları (IPRs), telif hakkı ve herhangi bir ortak çalışmanın korunması,
c) Üçüncü tarafların alt yüklenicileri ile birlikte bağlılığı ve altyüklenicilere uygulanması gereken güvenlik kontrolleri,

3.27.2. Antlaşmaların yeniden müzakeresi ya da feshi için şartları;

a) Taraflardan birinin antlaşmayı planlanan tarihten önce bitirmesi durumunda bir acil durum planı olmalıdır.
b) Kuruluş güvenlik gereklerinin değişmesi durumunda antlaşmaların yeniden müzakere edilmesi,
c) Varlık listeleri, lisanslar, antlaşmalar ve hakların geçerli belgeleri ve onlarla ilişkisi.

d) Farklı kuruluşlar ve farklı türdeki üçüncü taraflar arasında yapılan anlaşmalar önemli ölçüde değişebilir. Bu nedenle; anlaşmalar, belirlenen tüm riskleri ve güvenlik gereklerini içerecek şekilde yapılmalıdır. Gerektiğinde güvenlik yönetim planındaki gerekli kontroller ve prosedürler genişletilebilir.
e) Bilgi güvenliği yönetimi dış kaynaklı ise anlaşmalarda üçüncü tarafın güvenlik garantisinin yeterliliğini nasıl ele alındığı anlaşmada belirtilmelidir. Risk değerlendirmede tanımlandığı gibi, risklerdeki değişiklikleri belirlemek ve başa çıkmak için güvenliğin nasıl adapte edileceği ve sürdürüleceği ele alınmalıdır.
f) Dış kaynak kullanımı ve üçüncü taraf hizmet sunumunun diğer formları arasındaki farklılıkların bazıları; sorumluluk, geçiş durumu planlama ve işlemler süresince potansiyel kesinti süresi, acil durum planlaması yönetmelikleri ve durum tespitinin gözden geçirilmesi, güvenlik olayları hakkında bilgi toplanması ve yönetimi konularında sorular içerecektir. Bu nedenle, dış kaynaklı bir yönetmelik geçişinde; kuruluş değişiklikleri yönetmek için uygun süreçlere ve anlaşmaların yeniden müzakere edilmesi ya da fesh edilmesi hakkına sahip olduğu için kuruluşun planlaması ve yönetimi önemlidir.
g) Üçüncü taraflarla yapılan anlaşmalar diğer tarafları içerebilir. Üçüncü taraflara erişim hakkı verilmeden önce, erişim hakkı ve katılım için diğer tarafların ve koşulların belirlenmesi amacıyla anlaşmaya varılması gerekir.
h) Genellikle anlaşmaların esasları kuruluşlar tarafından geliştirilmiştir. Bazı durumlarda anlaşmaların üçüncü taraflarca geliştirilmesi ve kuruluşa empoze edilmesi durumu olabilir. Kuruluşlar, kendi yapılarına üçüncü taraflarca empoze edilecek anlaşmalarda kendi güvenliklerinin gereksiz yere etkilenmesini engeller.

3.27.3. Gizlilik Sözleşmeleri

Gizlilik veya ifşa etmeme anlaşmaları yasal olarak uygulanabilir terimleri kullanarak gizli bilgileri korumanın gerekliliğini ele almalıdır. Gizlilik veya ifşa etmeme anlaşmaları için aşağıdaki unsurlar dikkate alınmalıdır:

a) Korunacak bilginin bir tanımı (örneğin; gizli bilgileri),
b) Gizliliğin süresiz muhafaza edilmesi gereken durumlar da dahil olmak üzere anlaşma süresi,
c) Anlaşma sona erdiğinde yapılması gereken eylemler,
d) Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar ve imza eylemlerinin belirlenmesi (‘bilmesi gereken’ gibi),
e) Bilginin sahibinin, ticari sırların ve fikri mülkiyet haklarının ve bu gizli bilgilerin nasıl korunması gerektiği,
f) Gizli bilgilerin kullanım izni ve bilgileri kullanmak için imza hakları,
g) Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı,
h) Yetkisiz açıklama ya da gizli bilgilerin ihlal edilmesinin bildirimi ve raporlama prosesi,
i) İade veya imha anlaşmasına bırakılacak bilgi için terimler,
j) Bu anlaşmanın ihlali durumunda yapılması beklenen eylemler.
k) Bir kuruluşun güvenlik gereksinimlerine dayalı olarak, diğer unsurlarla bir gizlilik veya ifşa etmeme anlaşması gereklidir.
l) Gizlilik ve ifşa etmeme anlaşmaları uygulandığı yerin geçerli tüm yasa ve yönetmeliklerine uygun olmalıdır.
m) Gizlilik ve ifşa etmeme anlaşmaları için gerekler periyodik olarak veya gerekleri etkileyecek bir değişiklik olduğunda gözden geçirilmelidir.

n) Gizlilik ve ifşa etmeme anlaşmaları kurumsal bilgileri korumalı ve imzalayanın, bilginin korunmasından, kullanılmasından ve ifşa edilmesinden yetkili ve sorumlu olduğunu belirtmelidir.
o) Farklı koşullarda gizlilik ve ifşa etmeme anlaşmaları kuruluşun ihtiyaçları doğrultusunda farklı şekillerde kullanılmalıdır.

3.28. BULUT TEKNOLOJİLERİ POLİTİKASI

Bulut bilişim popülerliğini artırdıkça, bu yeni modelle ortaya çıkan güvenlik sorunları endişeleri artırmıştır. Geleneksel koruma mekanizmalarının etkinliği ve verimliliği yeniden değerlendirilmektedir, bu yeni yerleştirme modelinin özellikleri büyük ölçüde geleneksel mimarilerden farklılık arz etmektedir.

Özel bulut ekipmanlarının fiziksel kontrolünün yapılabilirliği ekipmanların tesis dışında ve başkalarının kontrolünde olmasından daha güvenlidir. Veri bağlantılarının güvenliği için fiziksel kontrol ve veri bağlantılarını görsel olarak incelemek ve portlara erişebilmek gereklidir. Bulut bilişimin benimsenmesi yolundaki engellerin sebebi çoğunlukla kamu ve özel sektörünün güvenlik tabanlı hizmetlerinin harici yönetiminin korku ve endişeye sebep olmasıdır. Bulut bilişim tabanlı hizmetlerin dışarıdan sağlanması ise en temel özelliğidir. Bu durum bulut bilişim hizmet sağlayıcılarına güvenli hizmetlerin yönetimini kurma ve sürdürmeye öncelik verilmesi hususunda iticidir.

a) Fiziksel Güvenlik Sunuculara erişimlerinin fiziksel olarak güvenliğinin en az TIER-3 seviyesinde sağlanmalıdır.
b) Network Güvenliği Network ekibi tarafından sağlanacak güvenlik tedbirleri refere edilmelidir.
c) Data Güvenliği;
d) Kriptografi: Veriyi korumanın yollarından biri de şifrelemedir. Bugün şifreleme çalışmaları oldukça ilerlemiş, bilgisayarlar oldukça gelişmiştir. Fakat bu durum saldırganlar için de geçerlidir. Hassas bilgiler bilinen ve test edilmiş şifreleme yöntemleri ile saklanmalıdır. Ayrıca daha önce kırılması uzun zaman alan algoritmalar günümüzde daha kısa zamanda çözülebilmektedir. Dolayısıyla uygulama içindeki algoritmalar zamanla gözden geçirilmeli ve güncellenmelidir.
e) Kimlik Erişim Yönetimi; yetkisiz erişimlerin tespiti ve ağ sistemlerinin korunması için gerekli kontrol faaliyetleri sağlanmalıdır.

3.29. UYGULAMA GÜVENLİĞİ;

a) Konfigürasyon Yönetimi; Konfigürasyon, uygulama ile ilgili hassas bilgileri içermektedir. Örnek vermek gerekirse veri tabanına erişim için gerekli bağlantı bilgilerini içeren dosyalar bu kapsamdadır. Konfigürasyona müdahale uygulamanın işleyişini değiştirebilir veya çalışmamasına sebep olabilir. Konfigürasyon dosyalarının sunucularda saklanıyor olması yeterli güvenlik önlemlerinin alındığı anlamına gelmemektedir. Konfigürasyon dosyaları hassas bilgi olarak nitelendirilmeli, şifrelenmiş bir şekilde tutulmalı ve bu dosyalara erişim kayıt altında tutulmalıdır.
b) Hassas Bilgi (Sensitive Information); Hassas bilginin ne olduğunun belirlenebilmesi için uygulamanın ve işin bir arada ele alınması gereklidir. Uygulama geliştirici işin niteliğini tam olarak bilemediğinden, diğer yandan işin sahibi de uygulamanın teknik altyapısı hakkında sınırlı bilgiye sahip olacağından bu iki taraf tek başlarına hassas bilgi için yeterli tanımlama yapamayacaklardır. İki tarafın bir araya gelmesiyle hassas bilgileri içeren bir liste oluşturulmalı ve bu listeyi koruyacak bir politika oluşturulmalıdır.
c) Kayıt Tutma ve Denetim; Uygulama veya uygulamanın yöneticileri saldırı altında olduklarını anlamalıdır. Bu durum aslında neyin normal neyin anormal olduğunun belirlenmesi ile sağlanır. Bir uygulamaya ilişkin normal süreç ve şablon tanımlanmalı ve bunu dışında bir olay olduğunda saldırı ihtimali ele alınmalıdır. Örneğin, normal senaryoda bir uygulamaya dakikada ortalama beş kişinin erişmesi beklenirken bu sayı bine ulaşıyorsa muhtemelen bir "Servis Dışı" bırakma atağı söz konusudur.

3.30. MOBİL CİHAZ GÜVENLİĞİ POLİTİKASI

Bilgiyi taşımanın kolay bir yolu laptop ve akıllı telefonlar gibi mobil cihazlardır. Bu cihazlarda bulunan hassas bilgiler ve erişim yetkileri de düşünüldüğünde mobil cihazlarda güvenliğin dikkat edilmesi gereken bir konu olduğu anlaşılmaktadır.

a) Mobil cihazlara erişimde mutlaka parola kullanılmalıdır.
b) Mobil cihazınızda ne tür bilgiler sakladığınızın farkında olun, hassas ve gizli bilgileri mümkün olduğunca mobil cihazınızda bulundurmayınız.
c) Verilerinizin yedeklerini alın ve güncel bir kopyasını farklı bir yerde saklayınız.
d) Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

3.31. İHLAL BİLDİRİM VE YÖNETİMİ POLİTİKASI

a) Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.
b) Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.
c) Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.
d) Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.
e) İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.
f) Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.
g) Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor edilir.
h) Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınır.
i) Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.
j) İç problem analizi, adli incelemeler veya üretici firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.
k) Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.
l) Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.
m) Kanıt toplama; kuruluş içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;
    a. Kanıtın mahkemede kullanılıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi,
    b. Kanıtın niteliği ve tamlığını gösteren ağırlığı.
n) Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:
    a. Uyarma
    b. Uyarma,

c. Kınama,
d. Para cezası,
e. Sözleşme feshi.

4. BİLGİ GÜVENLİĞİ İZLEME VE DENETLEME YÖNETİMİ

a) Bilgi Güvenliği Sistemi düzenli olarak denetlenmesi sağlanmalıdır.
b) Kurum yetkilileri tarafından Bilgi Güvenliği İç Denetimleri yapılmalıdır.
c) Hazırlanacak Bilgi Güvenliği İç Denetim soru listeleri hazırlanmalıdır.
d) Denetim yapacak personelin Bilgi Güvenliği konusunda yetkilendirilmiş kurumlardan iç denetim eğitimi almaları, denetime katılacak kişilerin iç denetçi sertifikasının olması gerekir.
e) İç denetimler için bütün birimleri kapsayacak şekilde denetim planı hazırlanmalıdır.
f) Denetim sonuçları iç denetim raporu şeklinde hazırlanmalı ve üst yönetime sunulmalıdır.
g) Denetimlerde tespit edilen bulgular için çözüm önerileri geliştirilmelidir.
h) Bir sonraki yapılacak iç denetimlerde, bir önceki tespit edilen bulguların çözümlenip çözümlenmediği hususunda takip yapılmalıdır.

4.1. Bilgi Güvenliği Testleri

a) Kılavuzda belirtilen standartların uygulanmasının kontrolleri hususunda yıllık plan yapılmalı, bu plan ile takvim günleri belirlenmelidir.
b) Belirlenen yıllık plana uygun olarak kullanıcı seviyesinde, yöneticiler seviyesinde, sistem yürütücü ekip seviyesinde, makineler seviyesinde, network seviyesinde gerekli kontroller, testler yapılmalıdır.
c) Yapılan kontrol, testler sonucunda çıkan sonuçlar puanlandırılarak raporlanmalıdır. Rapor içeriğindeki ilgili bölümlerin puanlandırma seviyesine göre gerekli hallerde ek farkındalık eğitimleri, seminerler verilmelidir. Makine ve network sistemi için gerekli görülen ek ayar düzeltmeleri yapılmalıdır.
d) Puanlandırma sisteminin oluşturulmasında sahadan Bilgi Güvenliği Kılavuzuna uygun olarak oluşturulmuş formlara belirlenecek personel tarafından veri bildirimleri girdirilmeli ve bu formlara uygun olarak yılın belirlenecek zamanlarında formlara uygun olarak oluşturulacak puanlamaların fiziksel kontrolleri sağlanmalıdır.
e) Yapılacak kontroller ve testler ISO 27001 sistemine, TÜBİTAK UEKAE, Siber Güvenlik Enstitüsü standartlarına bağlı kalınarak yürütülmelidir

4.2. Veri Merkezi Standartları Yönetimi

a) Kurumun veri merkezinde yedek enerji ve soğutma sistemleri olmalıdır.
b) Kurumun veri merkezi (Sistem odaları) yangın söndürme sistemlerine sahip olmalıdır. Yangın söndürme çözümleri veri merkezinde bulunan elektronik cihazlara ve personel sağlığına zarar vermeyecek şekilde olmalıdır. Bu yüzden bu özelliğe sahip gazlar kullanılmaktadır. Yangın söndürmede FM200, FE25, Argon ve Novec 1230 gazları kullanılmalıdır.
c) Kurumun veri merkezi olarak kullanılacak odalarda dışarıya açılan pencere veya kapı (balkon kapısı) bulunmamalıdır. Girişler için sadece tek kapı bulunmalıdır ve bu kapıda da gerekli güvenlik tedbirleri (biometric giriş, card-reader, şifre paneli) alınmış olmalıdır. Veri Merkezine yetkisiz personelin girişi engellenmelidir.
d) Veri Merkezi 7/24 güvenlik kameraları ile gözetlenmeli ve kayıt altına alınmalıdır. Oluşabilecek istenmeyen bir durumda 7/24 izleme yapan personeller öneme göre sorumlu personelle irtibata geçmeli ya da kendisi veri merkezine müdahale edebilecek yakınlıkta olmalıdır. Veri Merkezinde

bulunan iklimlendirme sistemlerinden sızan su sızıntıları, sıcaklık, yangın, voltaj değişimleri ve içeride bulunan havanın neminin izlenmesi amacıyla anlık bilgilendirme yapabilen sistemler ile takip edilmelidir. Bu bilgilendirmeler mail ve ya sms yoluyla sorumlu kişiye iletilebilmelidir.

e) Veri Merkezi için 7/24 güvenlik personeli bulunmalı ve tesisin fiziksel güvenliğini sağlamalıdır.
f) Veri Merkezine yapılacak tüm giriş ve çıkışlar kayıt altına alınmalıdır. İlgili personel tarafından, giriş yapan kişilerin bilgileri ayrıca log'lanmalıdır. (imzalı kayıt defteri gibi).
g) Veri merkezinde çalışacak personeller Veri Merkezi yönetimi konusunda yetkin olmalı ve gerekli durumlarda ilgili personele teknik ve farkındalık eğitimleri verilmelidir.
h) Veri merkezinde bulunan bütün güvenlik, acil durum ve iklim sistemlerinin periyodik bakımları yapılmalı ve bu bakımlar dokümante edilmelidir.
i) Veri merkezi içerisinde, sunucu yönetimi uzak masaüstü veya SSH gibi protokoller kullanılarak yapılmalıdır.
j) Veri merkezi içerisinde, acil durumlarda ya da felaket anında ki görev ve sorumluluklar belirlenerek dokümante edilmelidir.
k) Veri Merkezi Zemin Döşemesi kablo kanallarına ve soğuk hava akışına imkân verecek şekilde uygun bir yükseklikte (asgari 50 cm) yapılmalıdır.
l) Kullanılacak döşeme malzemeleri kabinlerdeki tam dolu olma durumu göz önünde tutularak 1000 kg kadar basınca dayanabilecek sağlamlıkta seçilmelidir. Günümüz kabinlerinin 1500 kg kadar yük taşıma kapasitelerine sahip olabildikleri göz önünde bulundurulmalıdır. Zemin altında karoları tutan destek ayakları mümkün olduğunca kabin ayaklarının basacağı noktaların altına veya yakınına konarak kabin yüklerinin taşınması kolaylaştırılmalıdır. Kabinlerin sallanması gibi ihtimallere karşı bu ayaklar yerlerinden kolayca oynamayacak ve birbirine destek olabilecek şekilde yerleştirilmelidir. Ayrıca kabinler için Deprem Ayağı da konulmalıdır.
m) Veri Merkezinde, sunucu kabinler ve kablolama işleri aşağıdaki standartlar çerçevesinde olmalıdır.
n) UTP, fiber ve enerji kablolarını birbirinden ayırmak için kanallar kullanılmalıdır. Kablolar birbirinin manyetiğinden etkilenmemelidir. Yanmaz kablolar tercih önceliğine sahip olmalıdır.
o) Kablo sonlandırmaları olabildiğince sağlıklı yapılmalı gerekirse sonlandırma yapıldıktan sonra kabloda performans ölçme cihazlarıyla test yapılmalıdır.
p) Manyetik alanın yüksek olacağı yerlerde mutlaka fiber kablo kullanılmalı, manyetik alandan etkilenmediği için böyle noktalarda verileri fiber ile taşımalıdır.
q) Kablolar döşenirken kıvrılmalara izin verilmemeli, 90 derecelik keskin dönüşler daha yumuşak şekilde yapılmalıdır. Kabloların kırılmalarını veya dışlarındaki muhafazasına zarar verecek keskin kenarlar üzerinden geçmelerini engelleyecek malzemeler kullanılmalıdır.
r) Kabinler yerde sabit ayaklarda durmaları küçük sarsıntılarda ileri geri hareket etmelerini engelleyecek bir yapı oluşturulmalıdır. Deprem gibi durumlarda devrilme yer değiştirme gibi ihtimaller düşünülerek yerleşim yapılmalı, kablo bağlantıları çok gergin tutulmamalıdır.
s) Kabin kapakları şifreli olmalı yetkisiz personel tarafından açılmamalıdır.
t) Gerek elektrik gerek data kablolarında mutlaka ana bağlantıların yedekli olarak çekilmesine önem verilmelidir. Kabloların yedekliliğinin yanında yedek kabloların sistem odasına farklı bir güzergâhtan girişlerinin sağlanmalıdır.
u) Sunucular doğru şekilde etiketlenmeli, sunucu kabinleri çalışma yapılmadığı zamanlarda kilitlenmelidir. Sunucu kabinlerinde kablolamalar düzgün ve kolayca ayırt edilecek şekilde yapılmalıdır. Bütün kablolar ayrı ayrı etiketlenmelidir.
v) Sunucular arası kablo bağlantıları yer altından yapılmalıdır.
w) Veri merkezi kurulumunda ve kurulum sonrasında periyodik olarak gerekli testler yapılmalı ve yapılan bu testler dokümante edilmelidir.

4.3. İletişim Ve İşletim Güvenliği Yönetimi

Bilgi sistemlerinin iletişim ve işletim görev ve sorumlulukları kuruluşun varlıklarının yetkisiz veya kasıtsız olarak değiştirilmesi ve yanlış kullanılmasını engellemek maksadıyla ayrılmalıdır. Hiçbir personel denetimsiz veya yetkisiz olarak sistemlere erişemez ve sistemleri değiştiremez.

4.3.1. Bilgi İşleme ve İşletim yönetimi aşağıda belirtilen konuları kapsar;

a) Bilgi işleme ve bulundurma gereksinimlerinin belirlenmesi,
b) Bilginin yedeklenmesi,
c) En erken işe başlama ve en geç işi tamamlama zamanlarının belirlenmesi,
d) Sistem kullanım kısıtları hata mesajlarını yöneten talimatların oluşturulması,
e) Beklenmeyen işletim ve teknik sorunlar karşısında destek irtibatları belirlenmesi,
f) Güvenli çıktı alma talimatlarının hazırlanması,
g) Sistem hatası durumunda yeniden başlatma ve kurtarma süreçlerinin belirlenmesi,
h) Sistem izleme kayıtlarının yönetiminin planlanması ve uygulanması.

4.3.2. Uygulama geliştirme, test ve operasyonel sistemlerinin ayrılması;

a) Yazılımın geliştirme sistemlerinden uygulama sistemlerine aktarımı kuralları belirlenmeli ve dokümante edilmelidir.
b) Geliştirme ve uygulama yazılımları ayrı işlemcilerde, ayrı sistemlerde, ayrı etki alanlarında veya kütüphanelerde çalıştırılmalıdır.
c) İhtiyaç olmadığı durumlarda operasyonel sistemlerde derleyici, editör, ve diğer geliştirme araçları bulundurulmaz.
d) Test sistemi operasyonel sistemle mümkün olduğunca aynı sistem olmamalıdır.
e) Kullanıcılar test ve uygulama sistemlerinde farklı kullanıcı tanımları kullanmalıdır.

4.3.2.1. Üçüncü taraflardan hizmet alımı esnasında gereken aktarımlar (bilgi, bilgi işleme imkânları ve taşınan diğer unsurlar) planlanmalı ve güvenlik daima göz önünde bulundurulmalıdır. Üçüncü taraf hizmetlerinin izlenmesi ve gözden geçirilmesi kapsamında;

a) Hizmet performans seviyesinin anlaşmaya uyumlu olduğu izlenmelidir.
b) Üçüncü tarafça hazırlanan hizmet raporları gözden geçirilmeli, anlaşmada belirtildiği şekilde geliştirme toplantıları yapılmalıdır.
c) Alınan hizmete ilişkin üçüncü taraf tarafından tutulan güvenlik olayları kayıtları, operasyonel sorunlar, hatalar, hizmet kesintileri gözden geçirilmelidir.
d) Varsa tespit edilen sorunlar yönetilmeli ve çözülmelidir.

4.3.2.2. Üçüncü taraf hizmetlerinde yapılan değişikliklerde;

a) Ağdaki değişimler,
b) Yeni teknolojilerin kullanımı,
c) Yeni ürünlerin daha yeni sürüm ve baskılara uyumu,
d) Yeni geliştirme araç ve ortamları,
e) Hizmetlerin verildiği fiziksel yerin değişimi göz önüne alınmalıdır.

4.3.2.3. Üçüncü taraflardan hizmet alımlarında değişiklik olması durumunda; kuruluş tarafından yapılan değişikliklerde;

a) Sunulan hizmetteki gelişmeler,

b) Yeni uygulama ve sistemlerin geliştirilmesi,
c) Kurumun politikalarındaki değişiklik ve güncellemeler,
d) Güvenliği geliştirmek ve bilgi güvenliği olaylarını çözmek için geliştirilen yeni kontroller göz önüne alınmalıdır.

e) Bilgi işlem teçhizatının kapasite yönetimine ilişkin olarak anahtar konumundaki sistem kaynaklarının kullanım durumu sistem yöneticileri tarafından sürekli izlenir, her yeni veya devam eden faaliyetin kapasite gereksinimi belirlenir. Sistemden en uygun şartlarda verim almak için sistem ayarları sürekli kontrol edilir. Gelecekteki sistem ihtiyaçları, ileriye yönelik planlanan yeni iş uygulamaları ve mevcut kapasite göz önüne alınarak değerlendirilir.

4.3.3. Ağ güvenliği;

a) Mümkün olduğu takdirde ağdan sorumlu personel bilgisayar işletiminden sorumlu personelden ayrı görevlendirilmelidir.
b) Uzak cihazların yönetimiyle ilgili sorumluluklar belirlenmelidir.
c) Halka açık ağ veya kablosuz ağlardan iletilen verinin bütünlüğünü sağlayacak tedbirler alınmalıdır.
d) Güvenlikle ilgili olayların kaydedilmesini sağlayıcı uygun izleme yöntemleri kullanılmalıdır.
e) Hizmet kalitesini artırmak ve bilgi işleme altyapısının sürekli kontrolünü sağlamak için yönetim faaliyetleri yakından koordine edilmelidir.
f) Ağ hizmetlerinin güvenli bir şekilde verildiği düzenli olarak izlenmelidir.
g) Ağ güvenliği için yetkilendirme, kriptolama, bağlantı kontrolü vb. güvenlik tedbirleri uygulanmalıdır.
h) Gerekli görüldüğünde ağ kullanımına sınırlar getirilmelidir.
i) Özellikle sağlık bilgisinin iletildiği ağların kesintiye uğraması durumundaki riskler ayrıca değerlendirilmelidir.

4.3.4. Taşınabilir ortamların yönetimi;

a) İhtiyaç kalmadığında tekrar kullanılabilir ortamların içeriği tekrar düzeltilemeyecek hale getirilmelidir.
b) Gerek görüldüğünde kurumdan taşınan ortam için yetkilendirme yapılır ve kayıt altına alınmalıdır.
c) Tüm ortamlar üretici talimatında belirtildiği şekilde emniyetli ve güvenli ortamda saklanmalıdır.
d) Ortamın saklama kapasitesinden daha uzun bir süre saklanmasına ihtiyaç duyulan bilgi, aynı zamanda farklı bir ortam üzerinde de saklanmalıdır.
e) Veri kayıplarını engellemek maksadıyla taşınabilir ortamları kayıt altına alınmalıdır.
f) Çıkarılabilir ortam sürücüleri sadece iş ihtiyaçları için kullanılabilir hale getirilmelidir.
g) Taşınan medya üzerinde kişisel sağlık bilgisi yer alıyorsa mutlaka kriptolanmalıdır.

4.3.5. Ortamın imha edilmesi;

a) Hassas bilgi içeren ortamlar yakılarak, silinerek, parçalanarak güvenli ve emniyetli bir şekilde yok edilmelidir.
b) Üzerindeki hassas bilgiyi ayırmaktan çok ortamları toplu olarak güvenli bir şekilde imha etmek daha kolay olabilmekte olup, bu durum imha aşamasında göz önüne alınmalıdır.
c) Birçok kurum atık toplama ve imha etme hizmeti vermekte olup, böyle bir kurumun seçimi durumunda güvenlik açısından uygun kontroller geliştirilmelidir.
d) Mümkün olduğu takdirde imha işlemi kayıt altına alınmalıdır.

4.3.6. Bilgi işleme süreci aşağıda belirtilen hususları kapsar;

a) Bilgi belirlenen sınıflandırma seviyesine işlenmeli ve etiketlenmelidir.
b) Yetkisiz personelin erişimini önlemek için erişim kısıtlamaları konulmalıdır.
c) Veriyi alan yetkililer kayıt altına alınmalıdır.
d) Girdi verisinin tamlığı, işlemenin uygun şekilde tamamlandığı ve çıktı doğrulamasının yapıldığı garanti edilmelidir.
e) Çıktı için havuzda bekleyen verinin hassasiyetine göre korunması sağlanmalıdır.
f) Üreticinin belirlediği özelliklere göre ortamların saklanması sağlanmalıdır.
g) Kopyalanan ortamların yetkili alıcının dikkatini çekmek için açık bir şekilde işaretlenmesi sağlanmalıdır.
h) Yetkili alıcı listeleri ile dağıtım listelerinin belirli aralıklarla gözden geçirilmesi sağlanmalıdır.
i) Özellikle sağlık bilgisi fiziksel olarak çok iyi korunmalı ya da şifrelenmelidir.
j) Sistem dokümantasyonunun güvenliği;
k) Sistem dokümantasyonu güvenli bir ortamda saklanmalıdır.
l) Sistem dokümantasyonuna erişim uygulama sahibi tarafından yetkilendirilmeli ve minimum seviyede tutulmalıdır.
m) Halka açık ağlarda tutulan veya bu ağlar üzerinden gönderilen sistem dokümantasyonu uygun bir biçimde korunmalıdır.

4.3.7. Bilgi değişim esasları;

a) Bilgi değişiminin kopyalanması, değiştirilmesi, yanlış yönlendirilmesi ve imhasından korunması sağlayıcı tedbirler alınmalıdır.
b) Elektronik iletişim kullanılarak iletilen bilginin zararlı kodlara karşı korunması için tedbir alınmalıdır.
c) İletilen elektronik bilginin eklentilerinin korunmasına yönelik tedbir alınmalıdır.
d) Elektronik iletişimin uygun kullanımına ilişkin politika ve prensipler geliştirilmeli ve yayınlanmalıdır.
e) Riskleri göz önüne alarak kablosuz iletişim kullanımı ile ilgili kurallar belirlenmelidir.
f) Çalışanlar, sözleşme tarafları ve diğer kullanıcıların kurumu karalayıcı, sıkıntıya sokucu, ardı ardına zincir posta, haksız kazanç sağlama gibi faaliyetlere katılmama sorumlulukları ortaya konulmalıdır.
g) Bilginin gizliliği, bütünlüğü ve güvenilirliğini korumak için kriptografik tekniklerin kullanımı değerlendirilmelidir.
h) Ulusal ve uluslararası mevzuat dâhilinde tüm mesajları kapsayan iş yazışmalarının saklanması ve imhası ile ilgili kurallar belirlenmelidir.
i) Kritik ve hassas bilgi, yazıcılar, kopyalayıcı cihazlar, faks makineleri vb. cihazlar üzerinde bırakılarak yetkisiz kişilerin erişmelerine imkân verilmemelidir.
j) Elektronik imkânlar kullanılarak mesajların dış adreslere otomatik iletilmesine kısıtlar getirilmeli ve kontrol edilmelidir.
k) Telefonla görüşürken hassas bilginin ifşa edilmemesi, bilginin dinlenmemesi için tedbir alınmasına dikkat edilmelidir.
l) Yetkisiz personel tarafından tekrar dinlenebileceğinden, yanlışlıkla numara çevrilebileceğinden hassas bilgi otomatik cevap kayıtlarına, iletişim sistemlerine konulmamalıdır.
m) Personel faks makinelerinin dikkatsiz kullanımının bilgi güvenliği açısından verebileceği zararlar konusunda bilinçli olmalıdır.
n) Personel, yetkisiz bilgi toplamayı engellemek için demografik veri, e- posta adresleri, kişisel bilgi vb. kayıt edilmemesi konusunda bilinçli olmalıdır.
o) Personel faks ve fotokopi makinelerinin arıza yapması halinde hafızalarında bilgi kaldığı, onarılmayı müteakip bu bilginin basıldığı veya iletildiği konusunda bilinçli olunmalıdır.

4.3.8. Dış taraflarla yapılacak bilgi değişim anlaşmalarında aşağıda belirtilen hususlar göz önüne alınır;

a) Bilgi gönderme ve alımının kontrolü için sorumluluklar belirlenmelidir.
b) Gönderenin, gönderim ve alımla ilgili bilgilendirilmesi sağlanmalıdır.
c) İnkâr edilemezlik ve izlenebilirlik garanti edilmelidir.
d) Paketleme ve transfer için asgari teknik standartlar belirlenmelidir.
e) Emanet anlaşmaları yapılmalıdır.
f) Kurye belirleme standartları belirlenmelidir.
g) Bilginin kaybolması gibi bilgi güvenliği olaylarındaki sorumluluklar tayin edilmelidir.
h) Bilginin uygun şekilde korunduğunu garanti etmek maksadıyla karşılıklı mutabık kalınmış bir etiketleme sisteminin hassas ve kritik bilgi üzerinde kullanılması sağlanmalıdır.
i) Veri koruma, telif hakları ve lisans uyumlulukları için sorumlulukların sahibi belirlenmelidir.
j) Kriptografik anahtarlar gibi hassas bilginin korunmasında ihtiyaç duyulacak özel kontroller belirlenmelidir.

4.3.9. Fiziksel ortamların taşınması;

a) Güvenilir taşıma şekli ve kuryeler kullanılmalıdır.
b) Yönetim tarafından yetkili bir kurye listesi belirlenmelidir.
c) Kuryelerin kimliğini kontrol eden süreçler geliştirilmelidir.
d) Paketleme, içeriğin fiziksel hasarlardan yeterince korunmasını sağlayacak şekilde yapılmalıdır.
e) Hassas bilgi, kilitli kapların kullanılması, elden teslim, kurcalanmaya karşı korunmalı, gerekirse farklı yollardan parçalı olarak gönderim yöntemleri kullanılarak açığa vurulması veya değiştirilmesi önlenmelidir.

4.3.10. Elektronik mesajlaşma;

a) Mesajların yetkisiz erişim, değiştirilme veya hizmet engelleme saldırısından koruma, mesajın doğru adreslemesi ve iletiminin sağlanması, servisin genel güvenirliği ve kullanılabilirliği, elektronik imza vb. hukuki sebepler, anlık mesajlaşma veya dosya paylaşımı gibi halka açık dış servisleri kullanmadan önce onay elde etme, halka açık ağ erişimlerinde daha güçlü kimlik denetimi yapma konuları göz önüne alınır.
b) Uzmanlar arasında e-posta ile iletilen sağlık bilgisi mutlaka şifrelenmelidir.
c) VPN kullanıcılarına verilen şifreler e-posta yoluyla değil sms aracılığıyla gönderilmelidir.

4.3.11. Çevrimiçi işlemlerle ilgili güvenlik açısından aşağıdaki hususlar dikkate alınır;

a) İşlem içerisinde yer alan her iki tarafın elektronik imzalarının kullanımı,
b) Her iki tarafın kullanıcı yetkilendirmelerinin doğru olduğu ve doğrulandığı, işlemlerin güvenli olduğu, her iki tarafın gizliliğinin sağlandığı,
c) Tüm tarafların iletişiminin şifrelenmesi,
d) Tüm tarafların iletişim protokollerinin güvenli olması,
e) İş detaylarının saklandığı yerin herkes tarafından erişilemeyen bir yerde bulunması,
f) Uçtan uca elektronik imzanın kullanıldığı güvenli bir yetkilendirme,
g) Bilgi sistemlerinde herkese açık bilginin değiştirilmeden arşivlenmesi.

4.3.12. Erişim kontrolüne ilişkin olarak sistem kayıtları asgari aşağıdaki hususları kapsar;

a) Kullanıcı tanımları,
b) Sisteme giriş-çıkış tarihi, zamanı gibi ana faaliyetler,
c) Terminal kimliği ve mümkünse yeri,
d) Başarılı ve ret edilen sisteme erişim girişimleri,
e) Başarılı ve ret edilen veri ve diğer kaynaklara erişim girişimleri,
f) Sistem konfigürasyonundaki değişiklikler,
g) Ayrıcalıkların kullanımı,
h) Sistem olanakları ve uygulamalarının kullanımı,
i) Erişilen dosyalar ve erişim türü,
j) Ağ adresleri ve protokoller,
k) Erişim kontrol sisteminin verdiği uyarılar,
l) Anti virüs ve saldırı önleme sistemleri gibi koruma sistemlerin başlatılması ve sonlandırılması.
m) Bilgilerde yapılan güncellemelerde kayıtların önceki durumları ayrıca log'lanır ve arşivlenir.

4.3.13. Belgelendirme Yönetimi

a) Bilişim sisteminin yapısı ile bütün iş ve işlemler açıkça belgelenmeli ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir durumda olmalıdır.
b) İş akışları uygun şekilde belgelenmelidir.
c) Belgeleme, tarih belirtilerek yapılmalı ve yedek kopyaları güvenli bir yerde muhafaza edilmelidir.
d) Girdi türleri ve girdi form örnekleri belgelenmelidir.
e) Ana dosyalar ile diğer dosyaların içerik ve şekilleri belgelenmelidir.
f) Çıktı form örnekleri ve çıktıların kimlere dağıtılacağı belgelenmelidir.
g) Programların nasıl test edildiği ve test sonuçları belgelenmelidir.
h) Bütün program değişikliklerinin detayları belgelenmelidir

4.3.14. Sosyal Medya Güvenliği

a) Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.
b) Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.
c) Kuruma ait hiçbir gizli bilgi, yazı sosyal medyada paylaşılmamalıdır.

5. SOSYAL MÜHENDİSLİK SALDIRILARI

Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanmaktadır. Başka bir tanım ise; İnsanoğlunun zaaflarını kullanarak istediğiniz bilgiyi, veriyi elde etme sanatına sosyal mühendislik denir. Sosyal mühendisler teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanların zaaflarından faydalanıp, en çok etkileme ve ikna yöntemlerini kullanırlar.

a) Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunmalıdır.
b) Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.
c) Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edilmelidir.
d) Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgileriniz paylaşılmamalıdır.
e) Şifre kişiye özel bilgidir. Sistem yöneticiniz dahil telefonda veya e-posta ile şifrenizi paylaşmamalısınız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.
f) Oluşturulan dosyaya erişecek kişiler ve hakları "bilmesi gereken" prensibine göre belirlenmelidir.

g) Erişecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.
h) Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.
i) Eğer paylaşımlar açılıyorsa ilgili dizine sadece gerekli haklar verilmelidir.
j) Kazaa, emule gibi dosya paylaşım yazılımları kullanılmamalıdır.

6. DEĞİŞİM YÖNETİM POLİTİKASI

Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.

a) Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.
b) Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve dokümante edilmelidir.
c) Değişiklikler gerçekleştirilmeden önce kurumun ilgili biriminden onay alınmalıdır.
d) Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.
e) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.
f) Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmelidir.
g) Teknoloji değişikliklerinin kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmeli ve dokümante edilmelidir.
h) Değişiklik yönetimini işletmek için bir talep yönetim sistemi kurmak ve işletmek önemlidir. Talebin nasıl alınacağı ve değerlendirileceği gibi esaslar tanımlanmalıdır.
i) Değişiklik onayının, "hangi kontroller ne şekilde yapıldıktan sonra verileceği" tanımlanmalıdır.
j) Değişiklik öncesi test süreci tanımlanmalıdır.
k) Değişikliğin varlık kritikliğine göre yapılacağı zaman ve yöntemler tanımlanmalıdır.

*****İstanbul Medipol Üniversitesi Bilgi Güvenliği Politikaları Kılavuzu 03/01/2017 Tarihli ve 2017/01-03 Sayılı Senato Kararı İle Yürürlüğe girmiştir.

Tablo (Ek-1)

Kısaltmalar Tablosu

Kısaltma	**Tanım**
Zincir e-posta	Bir kullanıcıya gelen şans ve para kazanma yöntemleri gibi bir içeriğe sahip e-postanın art arda diğer kullanıcılara gönderilmesi
Spam	Yetkisiz ve/veya istenmeyen reklam içerikli e-postalar
Sahte e-posta	Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenini kazanmak ve kişisel bilgilerine (tamamen yasadışı yoldan) erişmek
RADIUS (Remote Authentication Dial- in User Service)	Sunucular uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan internet protokolü
X.509/LDAP(Light weight Directory Access Protocol	Aktif dizin ve e-posta gibi programlardan bilgi aramak için kullanılan bir internet protokolü
Portal	Birden çok içeriği bir arada bulunduran alan
SSL (Secure Socket Layer)	Ağ üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş bir güvenlik protokolü
VPN	Bir ağa güvenli bir şekilde, uzaktan erişimi sağlayan teknoloji
IPSec (Internet Protocol Security) VPN	Genel ve özel ağlarda şifreleme ve filtreleme hizmetlerinin bir arada bulunduğu ve bilgilerin güvenliğini sağlayan iletişim kuralı ile uç kullanıcıya güvenli uzaktan erişim sağlama
IP	Bilgisayar ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alış verişi yapmak için kullandıkları adres
MAC adresi	Bir ağ cihazının tanınmasını sağlayan kendisine özel adres
SNMP	Bilgisayar ağları üzerindeki birimleri denetlemek amacıyla tasarlanmış protokol
Firmware	Sayısal veri işleme yeteneği bulunan her türlü donanımın kendisinden beklenen işlevleri yerine getirilebilmesi için kullandığı yazılımlar
DMZ	Kurum içi ağı ile kurum dışı ağı birbirinden ayıran bölge

Kısaltma	**Tanım**
Uzaktan Erişim	İnternet, telefon hatları veya kiralık hatlar vasıtası ile Kurumun ağına erişilmesi
Risk	Kurumun bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörler
Güvenli Kanal	Güçlü bir şifrelemeden oluşan iletişim kanalı
Uygulama Sunucusu	Dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımıdır. Üç katmanlı uygulamaların bir parçasıdır. Bu üç katman: Kullanıcı arayüzü (GUI), uygulama sunucusu ve veritabanı sunucusu
Yetkilendirme	Sisteme giriş izni verilmesi, çok kullanıcılı sistemlerde sistem yöneticisi tarafından, sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği işlemler için belirli izinler verilmesi
Yedekleme	Ekipmanın bozulması durumu düşünülerek dosyaların ve/veya veritabanının başka bir yere kopyalanması işlemi.
Veritabanı.	Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğu
Şifreleme	Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan özel bir algoritma
VLAN (Virtual LAN)	Sanal yerel ağ. Birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurmaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubu

Tablo (Ek-2)

Sunucu Adı	(.....)
IP Adresi	
Mac Adresi (Ethernet1) Mac Adresi (Ethernet2)	
Projenin Amacı	
Sunucunun Bulunduğu Birim Adı (Fiziksel Konum)	
Sorumlular (Yönetici Kullanıcıların Ad ve Soyadları)	
Ulaşılabilecek Telefon ve E-posta Adresi	Telefon: E-Mail:
Genel Donanım Özellikleri (Marka, Model, CPU, RAM, HDD)	
İşletim Sistemi	
Kullanıcı Kitlesinin Kimlerden Oluştuğu	
Yerel Kullanıcı Sayısı	
Tahmini Kurum Dışı Kullanıcı Sayısı	
Sunucu Üzerinde Bulunan Güvenlik Yazılımları	
Bünyesindeki Güvenlik Uygulamalarından Yararlanılmak İsteniliyorsa Erişime Açık Tutulması İstenen Servis Adları ve Port Numaraları	
Ek Açıklamalar	