1. AMAÇ

Bu politikanın amacı; Kurum'un (Osmanlı Yatırım Menkul Değerler A.Ş.) faaliyetlerinin ifasında kullandığı bilgi sistemlerinin yönetiminde esas alınacak ilkeler ile bilgi teknolojilerinin kullanımından kaynaklanan risklerin tanımlanması, ölçülmesi, izlenmesi, kontrol edilmesi, raporlanması ve yönetilmesine ilişkin esasları belirlemektir.

Kurum Üst Yönetimi, hız ve yenilikçiliği birleştiren müşteri odaklı hizmetlerinde, yüksek kalite ve verimliliği teminat altına almak amacıyla operasyonel hizmetleri sağlarken fayda-maliyet analizi ile dış kaynak ihtiyaçlarının belirlenmesi, bu tür kurumlardan alınan servisin verimli kullanımının ve yönetiminin sağlanması, tüm süreçlerindeki bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek, içeriden ve/veya dışarıdan gelebilecek kasıtlı ve kaza ile oluşabilecek tüm tehditlerden korunmasının sağlaması ve yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak gerçekleştirmesini hedeflenmektedir.

Bilgi Sistemleri, Bilgi Güvenliği ve Risk Yönetimi Politikası :

a) Bilgi Sistemleri Yönetimi

b) Bilgi Sistemleri Süreklilik Yönetimi

c) Bilgi Güvenliği Yönetimi

d) Bilgi Sistemleri Risk Yönetimi

süreçlerinde uygulanacak çerçeveleri belirlemektedir.

2. TANIMLAR VE KISALTMALAR

Bakım: Verilen servislerin devamlılığına yönelik olarak belirlenen periyotlarda Kurum veya ilgili firmalar tarafından sistem bileşenlerinin kontrol edilmesi, varsa sorunlu bileşenlerin normal çalışır duruma getirilmesi.

BGRYS: Bilgi Güvenliği ve Risk Yönetimi Sorumlusu.

Bilgi: Diğer önemli ticari varlıklar gibi, bir kurum için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi birçok biçimde bulunabilir. Kağıt üzerine yazılmış ve basılmış olabilir, elektronik olarak saklanmış olabilir, posta yoluyla veya elektronik imkanlar kullanılarak gönderilebilir, sunumlarda/filmlerde gösterilebilir veya karşılıklı konuşma sırasında sözlü olarak ifade edilebilir.

Bilgi Güvenliği: Bilginin**;**

Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunun sağlanması;

Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunun ve bütünlüğünün sağlanması;

Kullanılabilirlik(Erişilebilirlik): Yetkili kullanıcıların; gerek duyulduğunda, bilgiye ve ilişkili kaynaklara erişebilmelerinin sağlanması;

unsurlarının temini; ekipmanların, yazılımlar ve diğer bilgi teknolojisi varlıklarının korunmasıdır.

Bilgi Güvenlik Aksiyon Planları: Gap analizi/risk analizi sonucu risklerin minimuma indirilmesi, mevcuttaki politika ve standartlara uyum sağlanabilmesi ve/veya denetim faaliyetleri sonucu tespit edilen bulguların düzeltilmesi amacı ile yapılacak işlemler/çalışmalardır.

Bilgi Güvenlik İhlali: Bilgi güvenlik politikalarını, standartlarını, prosedürlerini veya talimatlarını ihlal eden veya bununla ters düşen herhangi bir olay.

Bilgi sistemleri süreklilik planı: Faaliyetlerin sürdürülmesini sağlayan bilgi sistemleri servislerinin, bir kesinti durumunda sürekliliğinin sağlanmasına yönelik hazırlanan ve iş sürekliliği yönetim sisteminin bir parçası olan plan.

Birim Yönetimi: Kurum organizasyon yapısında Müdür veya Direktör ünvanını içine alan yönetsel grup.

Birincil sistemler: Faaliyetlerin yürütülmesini ve Tebliğ'de, Tebliğe ilişkin alt düzenlemelerde ve ilgili diğer mevzuatta Kurum için tanımlanan tüm sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilerin, elektronik ortamda güvenli ve istenildiği an erişime imkan sağlayacak şekilde kaydedilmesini ve kullanılmasını sağlayan ve Genel Müdürlük binasındaki veri merkezinde yer alan, altyapı, donanım, yazılım ve veriden oluşan sistemin tamamı.

BSK (Bilgi Sistemleri Komitesi) : İcra Kurulu Başkanı, İcra Kurulu Üyeleri, Proje ve Talep Yönetimi Koordinatörü ve Bilgi Sistemleri Direktörü'nün katılımında oluşan ve Projelerin önceliklendirilmesi ve değerlendirilmesi, kritik ve acil değişikliklerin gözden geçirilmesi ve onaylanması konularında yetkili komite.
Çağrı: Telefon, e-mail veya diğer kanallarla müşteriye sunulan servislerle ilgili gelen bildirim.

Değişiklik İsteği (Dİ): Kurum'un kullandığı servislerde, ürünlerde, sistemlerde, Dış Kaynaklardan temin edilen uygulama yazılımlarında veya bunların dokümanlarında, değişiklik yapılmasını istemeye yetkili Kurum bölümleri/birimleri tarafından üründen sorumlu firmaya gönderilen değişiklik talebidir.

Donanım: Bilgi işlemeye yarayan bilgisayar veya telekomünikasyon aygıtları.

Dosya: Herhangi bir depolama ortamında saklanan kayıtlar topluluğu.

DÖF: Düzeltici ve Önleyici Faaliyet

E-posta: Elektronik-posta; herhangi bir ağ üzerinden kullanıcıların birbirine elektronik olarak mesaj ve/veya dosya gönderme/alma sürecini ifade etmek için kullanılan terminoloji.

Felaket: Faaliyet veya sistemlerde uzun süreli kesintiye sebep olabilecek düzeyde insan, doğa veya diğer faktörlerden kaynaklanan olay.

Güncelleme: Kullanılmakta olan ürünler için üreticileri tarafından yayınlanan yazılım değişikliklerinin, yama vb nin uygulanması.

Hassas Bilgi: Yönetimin isteği dışında açığa çıkması ile, Kurum ve müşterilerine ciddi stratejik ve finansal zararlar verebilecek veriler.

İkincil merkez: İkincil sistemlerin kullanıma hazır olacak şekilde tesis edildiği ve herhangi bir kesinti durumunda personelin çalışmasına imkan tanıyacak ve birincil merkez olan Genel Müdürlük ile aynı riskleri taşımayacak şekilde oluşturulan lokasyon.

İkincil sistemler: Birincil sistemler aracılığı ile yürütülen faaliyetlerde bir kesinti olması halinde, bu faaliyetlerin iş sürekliliği planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesini ve Tebliğ'de, Tebliğe ilişkin alt düzenlemelerde ve ilgili diğer mevzuatta Kurum için tanımlanan tüm sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istenildiği an erişilmesini sağlayan, Ankara'da ikinci bir lokasyondaki veri merkezinde bulundurulan birincil sistem yedekleri.

İşletim Sistemi: Bilgisayarların işletim fonksiyonları ile çalışmasını sağlayan yazılım.

İş sürekliliği planı: İş sürekliliği yönetiminin bir parçası olarak kesinti durumları için Kurumun öncelikleriyle uyumlu olarak engelleyici önlemler almayı, faaliyetlerin sürdürülmesine ve mevzuata uyum sağlanmasına yönelik politika, standart ve prosedürlerden oluşan ve Yönetim Kurulu tarafından onaylanan yazılı planlar.

İş sürekliliği yönetimi: Felaket, kriz veya kesinti durumunda etkin önlem alınabilmesi; itibarın, marka değerinin, değer yaratan faaliyetlerin ve paydaşların çıkarlarının korunabilmesi amaçlarıyla belirlenen operasyonların sürekliliğinin temin edilmesi veya hedeflenen zaman diliminde kurtarılabilmesinin sağlanması ve kriz öncesi duruma dönülmesine yönelik, potansiyel risklerin belirlenmesini de içeren politika, standart ve prosedürleri içeren bütünsel yönetim süreci.

Kaynak: Bilgi Sistemlerinde bulunan donanım, yazılım, veri (elektronik veya basılı).

Kesinti: Kurum faaliyetlerinde veya sistemlerinin fonksiyonlarında sürekliliğin, planlı geçişler haricinde mücbir sebeplerle sekteye uğraması.

Kurum Yönetimi: Organizasyon yapısında İcra Kurulu Üyesi, Genel Müdür, Genel Müdür Yardımcısı, Direktör, Müdür unvanlarını içine alan yönetsel grup.

Kullanıcı: Bilgi sistemlerine erişimi bulunan sistem kullanıcısı.

Kurum: Osmanlı Yatırım Menkul Değerler A.Ş.

Kurum Bilgi Sistemleri: Kuruma ait ve/veya yönetim sorumluluğu Kurum'da olan yazılım, donanım ve çevresel ekipmanının tümü.

Kurum Birimleri: Osmanlı Yatırım Menkul Değerler A.Ş. müdürlükleri.

Kişisel Bilgisayar (PC): Tek kullanıcı için dizayn edilmiş bilgisayar veya iş istasyonu.

Planlı Değişiklik: Önceden planlanmış ve Bilgi Sistemleri Prosedürü'nün Değişiklik Yönetimi adımlarına uygun olarak onayı alınmış değişikliklerdir.

Plansız Değişiklik: Herhangi bir sorunun çözümüne yönelik olarak zorunlu yapılması gereken değişikliklerdir.

Profil: Kullanıcıların çalışma ortamında gerek makina, gerekse uygulamalar üzerinde yapabileceklerini düzenleyen kurallar bütünüdür.

Proje ve Talep Yönetimi Koordinatörü : Projelerin ve taleplerin BSK'da önceliklerinin değerlendirilmesi sürecini yöneten ve Proje/Talep envanterinin güncelliğini sağlamaktan sorumlu olarak belirlenmiş kişi.

Risk Değerlendirmesi: Bilgi ve bilgi işleme vasıtalarının/süreçlerinin zayıflıklarının; bilgi ve bilgi işleme vasıtalarına/süreçlerine karşı var olan tehditlerin değerlendirilmesi; bu tehditlerin ortaya çıkma olasılıkları, oluşma sıklıkları ve etkilerinin tespitidir.

Risk Yönetimi: Bilgi sistemlerini/süreçleri etkileyebilecek olan risklerinin; uygun bir maliyette tanımlanması, kontrol edilmesi ve en aza düşürülmesi veya ortadan kaldırılması sürecidir.

Servis Seviyesi Anlaşması (SSA): Kurumun aldığı hizmetlere ilişkin Dış Kaynak Firmalarının taahhüt ettiği asgari servis seviyelerinin ve diğer koşulların tanımlandığı sözleşme.

Tedarikçi: Kurum tarafından kullanılmakta olan ürünler, uygulamalar vb.lerini temin eden firmalar.

Yazılım: Bilgisayar donanımlarını kontrol eden programlardır. İki temel kategorisi vardır. Sistem yazılımı (bilgisayarın kendi çalışmalarını yöneten; örneğin, işletim sistemi ve fonksiyonları) ve uygulama yazılımı (kullanıcının özel görevlerini yerine getiren; örneğin, ofis, muhasebe, finansal yatırım uygulaması vb.)'dır.

Yazılım Envanter Tablosu: Dış Tedarik yolu ile temin edilen yada kurum içerisinde geliştirilen uygulama yazılımlarının, ilgili Bölüm/Birimin, yazılım değiştirme, kontrol, test ve kabul yöntemlerinin listelendiği envanterdir.

Yedekleme (Backup) : Orijinallerinde problem yaşandığında veya bozulduğunda elde bulunması gereken dosya kopyaları ve bu kopyaların kullanımına yönelik prosedürler.

3. KAPSAM, POLİTİKA ve SORUMLULUKLAR

3.1. KAPSAM

Bu doküman:

a) Kurum'un tüm bilgi sistemleri varlıklarını (bilgisayar sistemlerini ve diğer bileşenlerini) ve iletişim ağlarını;

b) Personel, çevresel ve fiziksel alanları;

c) Tüm Bilgi Sistemleri süreçleri/işleyiş ve yöntemleri (iletişim ve işletim süreçleri, bilgi güvenliği, risk yönetimi süreçleri, iş/BT devamlılık süreçleri vb.);

d) Dış kurum ve şahıslarla ilişkileri, kontratları, hizmet sağlayıcıları;

e) Kanun, Tebliğ ve Yönetmeliklere uyumu;

kapsamakta olup, bu alanlarda uygulanır.

3.2. POLİTİKA

Bilgi Sistemleri, Bilgi Güvenliği ve Risk Yönetimi Politikası Yönetim Kurulu tarafından onaylanarak yürürlüğe girer. Söz konusu politikaların isleyişi düzenli olarak gözden geçirilir ve gereksinimler doğrultusunda güncellenir.

3.2.1. BİLGİ TEKNOLOJİLERİ YÖNETİMİ POLİTİKASI

3.2.1.1. Kurum stratejilerine uygun olarak projelerin gerçekleştirilmesini sağlamak üzere Projelerin değerlendirilmesi, önceliklendirilmesi ve takibinden Proje Yönetim Ofisi sorumludur.

3.2.1.2. Proje Yönetim Ofisi Operasyonlardan sorumlu İcra Kurulu üyesine bağlı olarak faaliyet gösterir.

3.2.1.3. Sistem ve Uygulama Proje ve Talepleri Bilgi Sistemleri Yönetimi Prosedürüne uygun olarak yönetilir.

3.2.1.4. Kurum'un Bilgi Sistemleri ana veri merkezi Kurum Genel Müdürlüğünde yer almaktadır. Veri Merkezi İş Sürekliliği Planı ve Bilgi Güvenliği Prosedürlerinde detaylandırılan gereksinimleri karşılayacak teknik yeterlilik ve kapasiteye sahip olarak yönetilir.

3.2.1.5. Kritik hizmetlerin sürekliliğini sağlamak üzere tam kapasiteli ikincil bir veri merkezi Ankara'da oluşturulur.

3.2.1.6. Kurum Sistemlerinin kurulumu, yönetimi, izlenmesi ve kapasite yönetimi Bilgi Sistemleri Yönetimi tarafından gerçekleştirilir.

3.2.1.7. Bilgi Sistemleri, Bilgi Güvenliğinin yönetimi ve koordinasyon sorumluluğu için ihtiyaç duyulması durumunda Dış Kaynak kullanılır.

3.2.1.8. Kullanılmakta olan uygulamalara ilişkin yeni proje ve değişiklik talepleri ihtiyaç duyulması durumunda Dış Kaynak Firmalarından tedarik edilir ve ilgili Servis Seviyesi Anlaşmalarına uygun yönetilir.

3.2.1.9. Donanım, işletim sistemi, yazılım ve uygulamalara yönelik değişikliklerin yönetimine ilişkin detaylar ayrıntılı olarak tanımlanır.

3.2.1.10. Tedarik edilen sistem, donanım, yazılım ve uygulamalara ilişkin Bakım işlemlerinin Dış Kaynak Hizmeti alınan firmalar tarafından, Servis Seviye Sözleşmelerine uygun olarak gerçekleştirilmesi sağlanır.

3.2.1.11. Konfigürasyon Yönetimi, Bilgi Sistemleri Ekibi tarafından Bilgi Sistemleri Yönetimi Prosedürüne uygun olarak gerçekleştirilir.

3.2.1.12. Olay ve Problem Yönetimi, Bilgi Sistemleri Yönetimi Prosedürüne uygun olarak gerçekleştirilir.

3.2.2. BİLGİ SİSTEMLERİ SÜREKLİLİK YÖNETİMİ POLİTİKASI

3.2.2.1. İş Sürekliliğini sağlamak üzere İş Sürekliliği Planı hazırlanır.

3.2.2.2. İş Sürekliliği planını test etmek üzere test senaryoları hazırlanır.

3.2.2.3. İş Sürekliliği testi her yıl tekrarlanır.

3.2.2.4. Kritik hizmetlerin, herhangi bir veri kaybı yaşanmadan devamlılığını sağlamak üzere etkin bir yedekleme planı oluşturulur ve süreç, Yedekleme Prosedürüne uygun yönetilir.

3.2.2.5. Bilgi Sistemlerinin kesintisiz veya kabul edilebilir kesinti süresi içerisinde felaket ve/veya iş sürekliliği merkezi üzerinden çalışmasının sağlanabilmesine yönelik yatırımlar yapılır.

3.2.2.6. Bilişim Sistemlerinin kesintisiz çalışmasının sağlanması için aynı ortamda kümeleme veya uzaktan kopyalama veya yerel kopyalama pasif sistem çözümleri hayata geçirilir. Sistemler tasarlanırken minimum süreli iş kayıpları hedeflenir.

3.2.2.7. Acil durumlarda sistem kayıtları incelenmek üzere saklanır.

3.2.2.8. Güvenlik açıkları ve ihlallerinin raporlanması için kurumsal bir mekanizma oluşturulur.

3.2.2.9. Yaşanan acil durumlar sonrasında politika ve süreçler yeniden gözden geçirilir ve ihtiyaçlar doğrultusunda gerekli iyileştirmeler yapılır.

3.2.3. BİLGİ GÜVENLİĞİ POLİTİKASI

Bilgi Güvenliği Politikası :

a) Kurumsal bilginin gizliliği, bütünlüğü ve erişilebilirliğini korumak,

b) İş sürekliliğini sağlamak,

c) Kurum Bilgi varlıklarını oluşabilecek tehdit ve tehlikelerden korumak ya da en düşük seviyede etkilenmesini sağlamak,

d) Kurum Personelinde bilgi güvenliği farkındalığı oluşturarak, bilgi güvenliğini tehlikeye sokacak ihlal olaylarını minimum seviyeye indirmek,

e) Bilgi teknolojileri alanında meydana gelen gelişim ve değişime uyum sağlamak amacıyla dinamik bir yapı oluşturmak ve otoriteler ile iletişimleri artırmak,

f) Kurum Bilgi varlıklarına yönelik riskleri tespit etmek ve düzenli bir şekilde bu riskleri yönetmek,

g) Bilgi güvenliği ile ilgili tüm yasal mevzuata uyum sağlamak,

h) Bilgi güvenliğini sağlamak için gereken yönetsel ve teknolojik önlemleri almak,

i) Bilgi güvenliğinin Kurum için önemini vurgulamak,

j) Yönetimin bilgi güvenliğine verdiği önemi ve desteği ifade etmek

ve böylece Kurumun güvenini ve itibarını sarsacak durumları bertaraf etmek amacıyla oluşturulmuştur.

3.2.3.1. Bilgi Sistemleri Bilgi Güvenliğinin sağlanmasına yönelik uygulama detayları, Bilgi Güvenliği Prosedürü'nde tanımlanır ve Kurum Personeli tarafından uygulanması sağlanır.

3.2.3.2. Kurum içerisinden yada Dış Kaynak kullanılarak, Bilgi Güvenliği ve Risk Yönetimi Sorumlusu (BGRYS) belirlenir.

3.2.3.3. Bilgi Güvenliğinin sağlanmasına yönelik aşağıdaki bileşenlere ilişkin kurallar ve detaylar Bilgi Güvenliği Prosedüründe ayrıntılı olarak tanımlanır:

a. E-Posta kullanımı

b. Kurum genelinde Parola kullanımı

c. İşletim sistemlerinin güvenliğinin sağlanması

d. Son kullanıcıların Bilgi Güvenliğinin sağlanmasına yönelik görev ve sorumluluklar

e. Kurum sitemlerine zarar verebilecek yazılımların etkin bir şekilde kontrol edilmesine yönelik Antivirüs kullanımına ilişkin kurallar

f. İnternet Erişimi ve Kullanımına ilişkin detaylar

g. Sunucuların güvenliğine yönelik kurallar

h. Ağ Cihazlarının Güvenliğinin sağlanmasına yönelik kurallar

i. Ağ Yönetimi politikasına ilişkin detaylar

j. Sistemlere uzaktan erişimin sağlanması ve kablosuz iletişime ilişkin uygulama

k. Fiziksel Güvenliğin sağlanmasına yönelik uygulama detayları

l. Kimlik Doğrulama ve Yetkilendirmeye ilişkin uygulama detayları

m. Veritabanı güvenliğinin sağlanması

n. Sistemlere erişim sağlayıp işlem yetkisine sahip Personele ilişkin güvenlik uygulama detayları

3.2.3.4. Bilgi sistemleri ile, içerdiği verinin güvenli biçimde saklanması esastır. Bu çerçevede, veriler, güvenlik hassasiyet derecelerine göre sınıflandırılır, her bir sınıf için uygun düzeyde güvenlik kontrolleri tesis edilir.

3.2.3.5. Bilgi güvenliğinin temininde ve Kurum'un bilgi sistemlerine erişimde, kimlik doğrulama ve yetkilendirme mekanizmaları ile inkâr edilemezlik ve sorumluluk atama imkânlarını içeren teknikler kullanılır.

3.2.3.6. Bilgi sistemlerinin geliştirilmesi, test edilmesi ve işletilmesi süreçlerinde görevler ayrılığı ilkesi uygulanır. Bilgi sistemleri yönetim sürecinde görev alan bölüm ve çalışanların görev, yetki ve sorumlulukları yazılı olarak belirlenir. Görevler ayrılığı ilkesine uygunluk düzenli olarak test edilir; sonuçları Bilgi Güvenliği ve Risk Komitesi'ne raporlanır.

3.2.3.7. Faaliyetlerin yürütülmesi sırasında bilgi sistemleri aracılığıyla edinilen ve saklanan müşteri ve Kurum bilgilerinin gizliliğini sağlamak esastır. Müşteri bilgilerinin, yasalarla yetkili kılınmış merciler dışındaki taraflarla paylaşımına ilişkin uygulama esasları yazılı olarak belirlenir.

3.2.4. BİLGİ SİSTEMLERİ RİSK YÖNETİMİ POLİTİKASI

3.2.4.1. Üst yönetim, bilgi sistemlerinden kaynaklanan risklerin etkin biçimde ve yeterli kaynaklarla yönetildiğini takip etmek; gerekli aksiyonların alınmasını ve kaynakların tahsis edilmesini sağlamakla yükümlüdür.

3.2.5. Kurum, bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce olası riskleri değerlendirir ve bilgi sistemlerine ilişkin risk analizini tekrarlar.

3.2.6. Kurum Bilgi Sistemleri Risk Yönetimine ilişkin detaylar Bilgi Sistemleri Risk Yönetimi Prosedürü'nde tanımlanır ve ilgili politika ve prosedür çerçevesinde yönetilir.

3.2.7. Kurum düzeyinde Risk Yönetimi algı düzeyini sağlamak üzere üst yönetim desteği vurgulanır.

3.2.8. Risk yönetimi ile süreçlerde sürekli iyileştirmelerin yapılması için, yönetim ve çalışanların; yeterli seviyede bilgilendirilmesi sağlanır.

3.2.9. Bilgi sistemlerinin yapısının, Kurum'un ölçeği, faaliyetlerin ve sunulan ürünlerin niteliği, çeşitliliği ve stratejik hedefleri ile uyumlu olması; bilgi sistemleri ile içerdiği verinin güvenilir, doğru, eksiksiz, izlenebilir, tutarlı, erişilebilir ve ihtiyaçları karşılayacak nitelikte oluşturulması esastır.

3.2.10. Bilgi sistemleri yönetimi kapsamında alınacak Dış hizmetlere ilişkin risk analizi yapılır. Dış hizmetinin alımı süresince Kurum'un maruz kalabileceği riskler ve bunların düzeyi ile Dış hizmet kuruluşunun sağladığı hizmetin yeterliliği değerlendirilir ve belirli dönemlerde Bilgi Güvenliği ve Risk Komitesi aracılığıyla üst yönetime sunulur.

3.2.11. Bilgi sistemleri kullanılarak gerçekleştirilen ve Kurum faaliyetlerine ait kayıtlarda değişikliğe neden olan işlemlere ilişkin olarak yeterli detayda ve açıklıkta denetim izleri oluşturulur. Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli tedbirler alınır.

3.2.12. Uygulamaya konulan bilgi sistemlerinin; isleyişi, stratejik hedeflere uygunluğu, kontrollerin etkinliği ve yeterliliği, bilgi teknolojilerindeki gelişmeler de göz önüne alınarak düzenli olarak izlenir. Yeni bilgi sistemlerinin Kurum'da uygulanmasının, Kurum'un risk profili üzerinde yaratacağı etki değerlendirilir. Bu çerçevede, gerek duyulması halinde, bilgi sistemleri isleyişi revize edilir.

3.3. SORUMLULUKLAR (BİLGİ SİSTEMLERİ ORGANİZASYONU)

Bilgi Sistemleri Ekibi ilgili İcra Kurulu Üyesi'ne bağlı olarak süreçlerini yönetir.

3.3.1. Bilgi Sistemleri Yönetimi

Bilgi Sistemleri Yönetimi;

a) Sistemlerin edinimi, kurulumu, yönetimi ve izlenmesi süreçlerini gerçekleştirir.

b) Uygulama değişikliklerinin test edilmesi sürecinde gerekli altyapıları sağlar.

c) Uygulama değişikliklerin gerçek ortama aktarılması sürecini koordine eder, gerçekleştirir.

d) Bilgi Sistemleri süreçlerinin Bilgi Sistemleri, Bilgi Güvenliği ve Risk Yönetimi Politikasına ve prosedürlere uygun yönetilmesini sağlar.

e) Yönetim Beyanı kapsamında yapılan iç denetim faaliyetlerine destek verir.

f) Yönetim Beyanı kapsamında yapılan iç denetiminde ortaya çıkan bulguların giderilmesi için gerekli planlama ve gerçekleştirme çalışmalarını yürütür.

g) Bilgi Sistemleri Bağımsız denetimi faaliyetlerinin gerçekleştirilmesine destek verir ve ortaya çıkarılan bulguların giderilmesini sağlar.

3.3.2. Bilgi Güvenliği ve Risk Komitesi

a) Kurum'un maruz kalabileceği bilgi teknolojilerine ilişkin risklerin ölçülmesi, ölçüm sonuçlarının raporlanması ve risk düzeyinin izlenmesi Bilgi Güvenliği ve Risk Komitesi sorumluluğundadır. Kurum'un bilgi sistemlerinden kaynaklanan riskler, Bilgi Güvenliği ve Risk Komitesi aracılığıyla üst yönetime raporlanır.

b) Üst yönetimin belirlediği strateji ve politikalar çerçevesinde, bilgi sistemlerinin risk yönetimi süreçleri, Bilgi Güvenliği ve Risk Komitesi tarafından yürütülür.

c) Yeni bilgi teknolojileri uygulamaya konulmadan önce, risk analizleri yapılmak üzere Bilgi Güvenliği ve Risk Yönetimi Sorumlusu'na iletilir. Yapılan risk analizi, yeni bilgi teknolojisinin kullanılacağı yeni ürün ve hizmete ilişkin nihaî risk değerlendirmesi yapılmak üzere Bilgi Güvenliği ve Risk Komitesi'ne iletilir.

d) Bilgi teknolojileri varlıklarının ve süreçlerinin süreklilik, kullanılabilirlik ve kurtarma yeteneklerini değerlendirmek ve güncel tutmak Bilgi Güvenliği ve Risk Komitesi'nin görevidir.

3.3.3. Proje Ofisi

a) Proje ve taleplerin envantere kaydedilmesini ve periyodik olarak Bilgi Sistemleri Komitesi (BSK) ve ihtiyaç duyulması durumunda İcra Kurulu'nun diğer üyelerinin katılımı ile değerlendirilmesi ve önceliklendirilmesi sürecine destek olur.

b) Proje ve Talep yönetiminin politika ve prosedürlere uygun yönetilmesi için gerekli kontrolleri gerçekleştirir ve ilgili birimlerin süreçlere uygun hareket etmesi için gerekli iyileştirme önerilerine ilişkin BSK'yı bilgilendirir.

c) Proje ve Taleplere ilişkin gereksinin dokümanının hazırlanmasını sağlar.

d) Yönetim Beyanı kapsamında yapılan iç denetim faaliyetlerine destek verir.

e) Yönetim Beyanı kapsamında yapılan iç denetiminde ortaya çıkan bulguların giderilmesi için gerekli planlama ve gerçekleştirme çalışmalarını yürütür.

f) Bilgi Sistemleri Bağımsız denetimi faaliyetlerinin gerçekleştirilmesi faaliyetlerinin koordinasyonunu sağlar.

3.3.4. BGRSY (Bilgi Güvenliği ve Risk Yönetimi Sorumlusu)

Bilgi Güvenliği ve Risk Yönetimi faaliyetlerinin koordinasyonunu sağlamak üzere Bilgi Güvenliği ve Risk Yönetim Sorumlusu atanır. BGRSY Kurum içerisinden atanır. BGRSY aşağıdaki sorumlulukları gerçekleştirir;

a) Kurum birimlerinin Bilgi Güvenliği Politikası ve Prosedürüne uygun olarak faaliyet göstermesi için gerekli desteği sağlar.

b) Gerektiğinde Kurum içi Bilgi Güvenliği ve farkındalığı eğitimlerinin alınmasını sağlar.

c) Yönetim Beyanı hazırlanması sürecinde İç Kontrol Birimlerine gerekli denetim desteği verir.

d) İç Denetim 'in Yönetim Beyanı kapsamında yapmış olduğu denetimlerde ortaya çıkan bulguların takip edilmesini ve BSK'nin bilgilendirilmesini sağlar.

e) Yıllık Bilgi Güvenliği Sızma Testlerinin gerçekleştirilmesi koordinasyonunu sağlar.

f) Sızma test sonuçlarına ilişkin aksiyonları hazırlar ve ilgili birimler tarafından bulguların kapatılması sürecini yönetir.

g) Gerektiğinde risk yönetimi ile ilgili periyodik eğitimler verilmesini sağlar.

3.3.5. BT İç Denetim Sorumlusu

a) Bilgi Teknolojilerine ilişkin iç denetim faaliyetlerinin planlanması, uygulanması ve tespit edilen bulgularının kapatılmasına ilişkin sürecin takip edilmesi ve yönetime raporlanmasını sağlar.

b) Yönetim beyanının hazırlanması sürecinde gerekli denetimleri gerçekleştirir ve hazırlanan raporu yönetim kuruluna sunar.

c) Bilgi Teknolojileri alt yapılarının (Donanım, Uygulama, Yazılım, Veritabanı Yönetim Sistemleri, İşletim Sistemleri,...) ve süreçlerinin belirli standartlar çerçevesinde işletildiğinin denetlenmesini sağlar.

d) İş süreçlerinin Bilgi Teknolojileri açısından incelenmesi ve varsa bilgi teknolojilerinin bu süreçleri destekleyecek şekilde iyileştirilmesi yönünde raporların hazırlanmasını sağlar.

e) BT risklerinin tespit ve değerlendirilmesi sürecine katkı sağlar.

f) BT yatırımlarının ve uygulamalarının etkin ve doğru maliyet yapısında tatbikinin incelenmesi ve teminini sağlar.

g) Risklerin iş sürekliliğini aksatmaması için gerekli önlemlerin alınması sürecine destek sağlar.

h) BT risk yönetim kültürünün şirket içerisinde yerleştirilmesi sürecine destek sağlar.

i) BT Denetim sonuçlarının raporlanmasını sağlar.

j) Yapılacak BT Denetimleri öncesi ilgili şirket BT yöneticilerine rehberlik edilmesi ve 3. parti denetçileri ile koordinasyonun sağlanması sürecini yönetir.

3.3.6. BT İç Kontrol Sorumlusu

a) İç kontrol standartlarının uygulanması ve geliştirilmesi konularında çalışmalar yapar.
b) İç ve dış denetim raporlarını izleyip gerekli iyileştirmelerin yapılmasını sağlar.
c) İç Kontrol Sisteminin yılda en az bir kez değerlendirilerek alınması gereken önlemleri belirler.
d) Bilgi güvenliğinin ve doğruluğunun kontrol ve temini sürecine destek sağlar.

e) Risklerin iş sürekliliğini aksatmaması için gerekli önlemlerin alınması sürecine destek sağlar.

f) Yönetim beyanının hazırlanması sürecine destek sağlar.

g) Bilgi Teknolojileri süreçlerine ilişkin uygulanacak kontrol listesinin oluşturulmasını sağlar.

h) Bilgi Teknolojileri süreçlerinin politika ve prosedürlere uygunluğunun kontrolünü gerçekleştirir ve tespit edilen bulguların üst yönetime raporlanmasını sağlar.

3.3.7. BSK (Bilgi Sistemleri Komitesi)

Bilgi Sistemleri Komitesi, Bilgi Sistemlerinden Sorumlu İcra Kurulu Üyesi koordinasyonunda, İcra Kurulu Başkanı, İcra Kurulu Üyeleri, Proje ve Talep Yönetimi Koordinatörü, Bilgi Sistemleri Direktörü ve ihtiyaç duyulması durumunda Bilgi Güvenliği ve Risk Yönetimi Sorumlusu katılımından oluşur.

BSK aşağıdaki fonksiyonların gerçekleştirilmesini sağlar:

a) Uygulama ve Sistemlere ilişkin; Proje ve Taleplerinin alınması, değerlendirilmesi ve önceliklendirilmesi sürecini yönetir.

b) Acil Durum Planının uygulanması sürecini Acil Durum Planına uygun olarak yönetir.

c) Acil değişikliklerin gerçek ortama aktarılmasına ilişkin değerlendirme yaparak onay/red kararı verir.

d) Bilgi Sistemleri Politika, Prosedür ve ilgili dokümanlarının gözden geçirilerek güncellenmesini ve devamlılığını sağlar.

e) Onaylanmış dokümanların Kurumda yayınlanmasını sağlar.

3.3.8. Birim Yöneticileri

Birim yöneticileri Bilgi Sistemlerinin yönetilmesi sürecinde, bilgi güvenliği ve risk yönetiminin sağlanması için:

a) Bu doküman ve bilgi güvenliği ve risk yönetimine ilişkin hazırlanmış veya onaylanmış dokümanların (politika, prosedür, standart, talimat vb.) kendisi ve personeli tarafından uygulanmasını sağlar.

b) Biriminin görev aldığı süreçlerde, risk analizlerinin gerçekleştirilmesini sağlar.

c) Birimindeki iş tanımları ve hedeflerine, bilgi güvenliği ve risk yönetimiyle ilgili sorumlulukları ekleyerek personele duyurulmasını sağlar.

d) Personelin; bilgi güvenliği ve risk yönetiminin önemi ve gerekliliği hakkında bilgilendirilmesi, Kurumun politika, prosedür standartları, talimatları vb. konusunda ilgili eğitimleri almasını sağlar.

3.3.9. İnsan Kaynakları Müdürlüğü

Bilgi Güvenliği ve Risk yönetiminin sağlanması için Birim Yönetimi sorumluluklarının yanı sıra:

a) Birim yöneticileri ile koordineli olarak personel sorumluluklarına bilgi güvenliği ve risk yönetimiyle ilgili sorumlulukların eklenmesini sağlar.

b) Performans değerlendirmelerinde birimlerin ve personelin bilgi güvenliği ve risk yönetimiyle ilgili olarak çalışmalarının dikkate alınmasını sağlar.

c) Yeni işe başlayan personelin bilgi güvenliği ve risk yönetimiyle ilgili dokümanlar(politika, standartlar, prosedürler vb.) ve sorumlulukları hakkında bilgilendirilmesini ve kayıt altına alınmasını sağlar.

d) BGRYS ile koordineli olarak ilgili personelin periyodik olarak bilgi güvenliği ve risk yönetimiyle ilgili eğitim almasını sağlar ve eğitim kayıtlarının saklanmasını temin eder.

3.3.10. Personel/Kullanıcı

Her çalışan bilgi güvenliği ve risk yönetiminin desteklenmesi için:

a) Onaylanmış bilgi güvenliği ve risk yönetimiyle ilgili politika ve prosedürlere uygun davranır; Kurum kaynaklarını bunlara uygun olarak ve işinin gerektirdiği şekilde kullanır; kişisel hedef ve iş tanımlarında belirtilen bilgi güvenliği ve risk yönetimi gereklerini yerine getirir.

b) Kendi çalışma alanlarındaki/ görev aldığı süreçlerdeki bilgi güvenliği ve risklerinin yönetilmesinden sorumludur.

4. REFERANSLAR / İLGİLİ DOKÜMANLAR

"Bilgi Sistemleri Yönetimi Prosedürü", PRS.BS.YON
"İş Sürekliliği Planı", PLN.BS.SUR

"Bilgi Güvenliği Prosedürü", PRS.BS.GUV

"Risk Yönetimi Prosedürü", PRS.BS.RSK

5. EKLER

Herhangi bir ek bulunmamaktadır.

6. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar
Rev 0.1	31.01.2018	Bilgi Sistemleri Yönetimi Tebliğine uygun olarak hazırlanan ilk sürüm.	Bilgi Sistemleri Komitesi
Rev 0.2	12.08.2019	Yıllık gözden geçirme kapsamında revize edilmiştir.	Bilgi Sistemleri Komitesi
Rev 3.0	11.12.2020	Yıllık gözden geçirme kapsamında revize edilmiştir.	Bilgi Sistemleri Komitesi