BİLGİ GÜVENLİĞİ POLİTİKASI

DOKÜMAN KODU	:	BSY-PL-01
HAZIRLAYAN/SÜREÇ SAHİBİ	:	ÜST YÖNETİM
KONTROL EDEN	:	YASAL UYUM
ONAYLAYAN	:	YÖNETİM KURULU
ONAY TARİHİ	:	27.10.2023
SON REV. TARİHİ	:	30.09.2025
VERSİYON NO	:	03
İLGİLİ DOKÜMANLAR	:	BİLGİ GÜVENLİĞİ POLİTİKASI BİLGİ GÜVENLİĞİ RİSK YÖNETİMİ POLİTİKASI PAROLA POLİTİKASI KİMLİK VE ERİŞİM YÖNETİMİ POLİTİKASI UZAKTAN ERİŞİM POLİTİKASI VERİ İMHA POLİTİKASI MOBİL CİHAZ GÜVENLİĞİ POLİTİKASI TEMİZ MASA TEMİZ EKRAN POLİTİKASI E-POSTA POLİTİKASI VERİ BÜTÜNLÜĞÜ POLİTİKASI BİLGİ SİSTEMLERİ GÖREVLER AYRILIĞI POLİTİKASI ANTİVİRÜS KULLANIM POLİTİKASI VARLIK YÖNETİMİ PROSEDÜRÜ AĞ GÜVENLİĞİ YÖNETİMİ PROSEDÜRÜ FİZİKSEL VE ÇEVRESEL GÜVENLİK PROSEDÜRÜ BİLGİ GÜVENLİĞİ İHLAL YÖNETİMİ PROSEDÜRÜ İŞ SÜREKLİLİĞİ ve ACİL DURUM EYLEM PLANI BİLGİ SİSTEMLERİ SÜREKLİLİK PLANI BİLGİ SİSTEMLERİ DIŞ KAYNAK YÖNETİMİ PROSEDÜRÜ YEDEKLEME PROSEDÜRÜ DEĞİŞİKLİK YÖNETİMİ PROSEDÜRÜ DENETİM İZLERİ YÖNETİMİ PROSEDÜRÜ YAMA YÖNETİMİ PROSEDÜRÜ PERFORMANS YÖNETİMİ VE KAPASİTE PLANLAMASI PROSEDÜRÜ PROJE YÖNETİMİ PROSEDÜRÜ UYGULAMA GELİŞTİRME PROSEDÜRÜ VERİ ŞİFRELEME VE ANAHTAR YÖNETİMİ PROSEDÜRÜ ZAMAN SENKRONİZASYON PROSEDÜRÜ BİLGİ SİSTEMLERİ İÇ KONTROL PROSEDÜRÜ

İÇİNDEKİLER

1. AMAÇ 3
2. KAPSAM 3
3. TANIMLAR 3
4. SORUMLULUK 5
5. POLİTİKA 9
5.1 BİLGİ SİSTEMLERİ RİSK YÖNETİMİ 10
5.2 BİLGİ SİSTEMLERİ KONTROLLERİNİN TESİSİ VE YÖNETİLMESİ 12
5.3 VARLIK YÖNETİMİ VE VERİ SINIFLANDIRMA 12
5.4 GÖREVLER AYRILIĞI İLKESİ 13
5.5 FİZİKSEL VE ÇEVRESEL GÜVENLİK 13
5.6 AĞ GÜVENLİĞİ 14
5.7 GÜVENLİK KONFİGÜRASYONU YÖNETİMİ 15
5.8 GÜVENLİK AÇIKLARI VE YAMA YÖNETİMİ 16
5.9 ZARARLI YAZILIMLARDAN KORUNMA 16
5.10 KİMLİK DOĞRULAMA 17
5.11 ERİŞİM YÖNETİMİ 18
5.12 İŞLEMLERİN, KAYITLARIN VE VERİLERİN BÜTÜNLÜĞÜ 18
5.13 VERİLERİN GİZLİLİĞİ 18
5.14 MÜŞTERİ BİLGİLERİNİN GİZLİLİĞİ 19
5.15 ÜÇÜNCÜ TARAFLARLA BİLGİ DEĞİŞİMİ 20
5.16 MÜŞTERİLERİN BİLGİLENDİRİLMESİ 20
5.17 BİLGİ SİSTEMLERİNE İLİŞKİN DIŞARIDAN ALINAN HİZMETLERİN YÖNETİMİ 20
5.18 KAYIT MEKANİZMASININ OLUŞTURULMASI 21
5.19 ZAMAN SENKRONİZASYONU 22
5.20 BİLGİ GÜVENLİĞİ İHLALİ 22
5.21 BİLGİ SİSTEMLERİ EDİNİMİ, GELİŞTİRİLMESİ VE BAKIMI 23
5.22 UYGULAMA GÜVENLİĞİ 24
5.23 BİLGİ SİSTEMLERİ GÜVENLİĞİ 25
5.24 DEĞİŞİKLİK YÖNETİMİ 26
5.25 BİLGİ GÜVENLİĞİ EĞİTİMLERİ 26
5.26 DENETİM VE KONTROL 27

1. AMAÇ

Bilgi Güvenliği Politikası (Politika), Neo Menkul Değerler A.Ş. (Neo/Şirket)'nin bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanmasını, bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin ve sorumlulukların tanımlanmasını, bilgi sistemlerine ilişkin risklerin yönetilmesine dair süreçlerin oluşturulmasını, kontrollerin tesis edilmesini ve gözetiminin sağlanmasını amaçlar.

2. KAPSAM

Bu Politika, bilgi/verinin depolandığı, aktarıldığı, işlendiği Şirket bilgi işlem altyapısını, bilgi işlem altyapısını barındıran fiziksel ortamları, bilgi işlem altyapısını kullanan tüm birim ve personeli, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsar.

3. TANIMLAR

APİ	Bir yazılımın başka bir yazılımda tanımlanmış işlevleri kullanabilmesi için oluşturulmuş uygulama programlama ara yüzü.
Bilgi Varlığı	Şirket'in Kanundan ve Kanuna ilişkin alt düzenlemelerden kaynaklanan görevlerini yerine getirmesi esnasında kullandığı veri ile bunların üretildiği, işlendiği, iletildiği ve saklandığı donanım ve yazılım unsurları.
Bilgi Güvenliği	Şirket varlıklarının gizlilik, bütünlük ve erişilebilirlik özelliklerinin korunması.
Bilgi Güvenliği İhlali	Bilgi sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesi veya teşebbüste bulunulması, siber olay.
Bilgi Sistemleri	Bilginin işlendiği, iletildiği ve saklandığı yazılım, donanım ve iletişim altyapısı ile bunlarla etkileşimde bulunan insan kaynağı, faaliyet ve süreçlerin tümü.
Birincil Sistemler	Şirket'in Kanundan ve Kanuna ilişkin alt düzenlemelerden kaynaklanan görevlerini yerine getirmesi için gerekli bilgilerin elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde kaydedilmesini ve kullanılmasını sağlayan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamı.
Bütünlük	Bilginin doğruluğu ve tamlığını koruma özelliği.
Çok faktörlü kimlik doğrulama	Kimlik doğrulama işleminin; kişinin bildiği, kişinin sahip olduğu veya kişinin biyometrik karakteristiği olan doğrulama faktörleri arasından iki veya daha fazla farklı faktörün kullanılarak gerçekleştirilmesi.
Denetim İzi	Bilgi sistemleri aracılığıyla gerçekleşen işlemlerin ve bilgi güvenliği ihlal olaylarının başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtlar ile bu kayıtlar üzerinde yapılan işlemleri gösteren kayıtlar.

Erişilebilirlik	Bilginin yetkili kullanıcı, uygulama veya sistem tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği.
Gizlilik	Bilgi sistemlerine ve bilgiye sadece yetkili kullanıcı, uygulama veya sistem tarafından erişilebilmesi.
Güvenli Alan	Bilgi işleme, iletişim ve depolama donanımlarını barındıran alan.
Hassasiyet	Şirket bünyesinde saklanan, müşterilere ait olan ve üçüncü kişilerce ele geçirilmesi halinde ilgili kişinin zarar görmesine, dolandırılmasına ya da sahte işlem yapılmasına sebep olabilecek verinin niteliği.
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 Kanunda ve Kanuna ilişkin alt düzenlemelerde Şirket için tanımlanan sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istenildiği an erişilmesini sağlayan birincil sistemin tüm yedekleri.
Kişisel veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Kişisel verilerin işlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Kanun	6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanunu
Kontrol	Bilgi sistemleri süreçleriyle ilgili olarak gerçekleştirilen ve iş hedeflerinin gerçekleştirilmesi, istenmeyen olayların belirlenmesi, engellenmesi ve düzeltilmesine ilişkin yeterli derecede güvenceyi oluşturmayı hedefleyen politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamı.,
Kritiklik	Bilgi varlığının, Şirket'in iş hedeflerine ulaşmasındaki önemini veya gerekliliğini belirten niteliği.
Kullanıcı	Şirket'in bilgi sistemlerinde kendisi adına hesap açılan Şirket personeli, dışarıdan hizmet sağlayıcının personeli veya Şirket'in müşterisi.
Kurumsal SOME	SOME Tebliği kapsamında Şirket tarafından kurulan Kurumsal Siber Olaylara Müdahale Ekibi.

Politika	Şirket'in hedef ve ilkelerini ortaya koyan ve yönetim kurulu veya üst yönetimi tarafından onaylanmış doküman.
Prosedür	Süreçlere ilişkin işlem ve eylemleri tanımlayan doküman.
SOME Rehberi	Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanmış en güncel "Kurumsal SOME Kurulum ve Yönetim Rehberi" dokümanı.
SOME Tebliği	11/11/2013 tarihli ve 28818 sayılı Resmî Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ.
Süreç	Bir işin yapılış ve üretiliş biçimini oluşturan sürekli işlem ve eylemler.
Uçtan Uca Güvenli İletişim	İletişime konu veriye sadece alıcısının erişebilmesi amacıyla, verinin gönderen tarafından sadece alıcının çözebileceği şekilde şifrelenerek iletilmesi.
USOM	Bilgi Teknolojileri ve İletişim Kurumu bünyesinde yer alan Ulusal Siber Olaylara Müdahale Merkezi.
Üçüncü Taraf	Şirket'e sözleşme ile hizmet sağlayan gerçek ve tüzel kişiler.
Üst Yönetim	Şirket Genel Müdürü, ilgili iş birimlerinin üst düzey yöneticileri ile Yönetim kurulu tarafından belirlenen diğer kişileri,
Varlık	Elektronik ve/veya fiziksel ortamlarda yer alan; iletişim yoluyla aktarılabilen bilgiyi içeren, Şirket'in iş süreçleri açısından değer taşıyan tüm bilgi ve bilgi işleme olanakları, bilgiyi kullanan ve taşıyan personel ile bilgiyi barındıran fiziksel mekânları,
Varlık Sahibi	Bilgi varlıklarına yönelik güvenlik gereksinimlerini belirleyen ve bu gereksinimlere uyumu gözeterek bilgi varlığının idamesi ve güvenliğinden sorumlu olan kişi veya birim.
Yama	Programlarda tespit edilen güvenlik açıkları veya programın içeriğindeki hatalı bir fonksiyonu düzeltme amaçlı hazırlanan program eklentisi

4. SORUMLULUK

Bu Politika kapsamındaki sorumluluklar aşağıda belirtilmiştir.

Yönetim Kurulu

- Bilgi sistemlerinin yönetiminin kurumsal yönetim uygulamalarının bir parçası olarak ele alınması.
- Bilgi sistemlerinin doğru yönetimi için gerekli finansman ve insan kaynağının tahsis edilmesi.
- Bilgi sistemleri güvenliğine ilişkin kontrollerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetimi hususunda üst yönetime

rapor veren ancak bilgi sistemleri yönetimine ilişkin gerekliliklerin yerine getirilmesi hususunda herhangi bir görevi bulunmayan, yeterli teknik bilgiye ve tecrübeye sahip bir bilgi güvenliği sorumlusu belirlenmesi.

- Bilgi Güvenliği Politikası'nın ve prosedürlerinin oluşturulması ve uygulanması faaliyetlerinin gerçekleştirilmesi; yılda en az bir defa, ayrıca önemli güvenlik olayları, yeni güvenlik açıkları ya da teknik altyapıdaki önemli değişikliklerden sonra gözden geçirilmesi.
- Bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğini sağlamak amacıyla bilgi sistemleri üzerinde etkin kontrollerin tesis edilmesinin sağlanması.
- Gelişen yeni teknolojileri de göz önünde bulundurarak bilgi sistemlerinin kullanımından kaynaklanan risklerin yönetilmesi için etkin bir gözetim yürütülmesi.
- Bilgi sistemleri strateji planı doğrultusunda bilgi sistemleri yatırımlarının uygun bir şekilde kullanılıp kullanılmadığının ve kurumun iş hedefleri ile bilgi sistemleri hedeflerinin birbiriyle uyumluluğunun gözetimi.
- Bilgi sistemleri üzerindeki risklerin etkin bir denetim ve denetim kayıt izi mekanizmalarının oluşturulması.
- Dışardan hizmet alımlarının doğuracağı risklerin değerlendirilmesi ve yönetilmesi.
- Bilgi sistemlerinin yılda en az bir kere sızma testine tabi tutulması ve bağımsız denetimine ilişkin dışarıdan hizmet alımının sağlanması.
- İç denetim ve iç kontrol planlarının onaylanması, uygulanmasının sağlanması;
- Sızma testi, denetim ve kontrol raporlarında yer alan bulgulara yönelik aksiyonların takibinin sağlanması.

Üst Yönetim

- Bilgi Güvenliği Politikası ve ilgili politika ve prosedürlerin uygulanmasının gözetimi.
- Bilgi sistemleri yönetimi konusunda rol ve sorumlulukların yazılı olarak belirlenmesi ve görevler ayrılığı ilkesi çerçevesinde görevlendirmeler yapılması.
- Şirket operasyonlarının istikrarlı, rekabetçi, gelişen ve g bir çizgide sürdürebilmesi için bilgi sistemlerine ilişkin stratejilerinin iş hedefleri ile uyumlu olmasının sağlanması.
- Personelin bilgi güvenliği ve gizliliği konusundaki farkındalık düzeylerinin artırılması, bilgi güvenliği farkındalığı eğitim programının onaylanması ve programın içeriğinin yılda en az bir defa yeni teknolojiler ve ortaya çıkan yeni riskler dikkate alınarak gözden geçirilip güncellenmesi.
- Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projelerin gözden geçirilmesinden; bunlara ilişkin risklerin yönetilebilirliği göz önünde bulundurularak onaylanmasından ve yönetsel rol ve sorumlulukların açıkça belirlenmesinden; tüm sorumlulukların her yıl gözden geçirilmesi ve onaylanması.
- Bilgi güvenliği önlemlerinin uygun düzeye getirilmesi hususunda gereken kararlılığı gösterip bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağın tahsis edilmesi.

- Dış hizmet olarak alınacak hizmetlerin Şirket açısından doğuracağı risklerin yeterli düzeyde değerlendirilmesi, yönetilmesi ve dış hizmet sağlayıcı ile ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayan yeterli bir gözetim mekanizması tesis edilmesi.
- Aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaların kurulması:

  a) Bilgi sistemlerine ve süreçlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve bu çerçevede söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetiminin gerçekleştirilmesi,
  b) Bilgi sistemlerinin sürekliliğinin sağlanması,
  c) Bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve her yıl değerlendirilmesi,
  d) Tüm çalışanların bilgi güvenliği farkındalığını artırmaya yönelik çalışmaların yapılması ve eğitimlerin verilmesi

- Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen süreç ve prosedürlerin, Şirket'in organizasyonel ve yönetsel yapısı içerisinde fiili olarak işleyecek şekilde yerleştirilmesi ve işlerliğine ilişkin gözetim ve takiplerin gerçekleştirilmesi.
- Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için, kritik iş süreçlerine ilişkin kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybını da içeren iş sürekliliği planı hazırlanması.
- Denetim ve iç kontrol raporlarında yer alan tespitlere göre alınacak aksiyonların onaylanması ve aksiyonlara uyumun sağlanması.

Bilgi Güvenliği Sorumlusu

- Bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesi ve takibi.
- Bilgi Güvenliği Yönetim Süreci'ne yönelik yapılan çalışmaların organize edilmesi ve yapılan çalışmalar hakkında Bilgi Güvenliği Komitesi'nin bilgilendirilmesi.
- Bilgi Güvenliği Politikası, prosedürleri ve süreç dokümanlarının oluşturulması, bunların güncellenmesi ve onaya sunulması.
- Bilgi güvenliği bakış açısıyla, bilgi varlıklarının sınıflandırılması ve bilgi varlıklarına yönelik gizlilik, bütünlük, erişilebilirlik kriterleri bakımından bilgi sistemleri risk yönetimi çalışmalarına aktif katkı sunulması ve yardımcı olunması.
- İlgili birimlerle uyum içinde, iş gereksinimleri ve iş hedefleriyle uyumlu Şirket genelinde bilgi güvenliğinin tesis edilmesi.
- Bilgi güvenliği ile ilgili mevzuat hükümlerine, standartlara, politika, prosedür ve süreç dokümanlarına uyumun takip edilmesi.
- Bilgi güvenliği faaliyetlerinin ve testlerinin yürütülmesinin sağlanması ve bunların takip edilmesi.
- Önemli projeler ve değişiklikler için bilgi güvenliği gereksinimlerinin belirlenmesi çalışmalarına katkıda bulunulması.
- Şirket'in bilgi güvenliğini ilgilendiren paydaşlara (çalışan, müşteri, ürün ve hizmet sağlayıcılar) yönelik bilgi güvenliği farkındalık programının yürütülmesi.

- Bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda Üst Yönetime rapor verilmesi.
- Şirket bünyesinde gerçekleşen her türlü bilgi güvenliği ihlal olayının ve bilgi sistemlerine ilişkin ortaya çıkan zayıflıkların yönetilmesini sağlayacak kontrollerin tesis edilmesi.
- Gerçekleşen ihlal veya ortaya çıkan zayıflığın mümkün olan en kısa sürede kayda alınması ve çözülmesi için gerekli mekanizmaların kurulmasından ve tüm personelin bilgilendirilmesi.
- Bilgi sistemlerinin kullanımına ilişkin kimlik doğrulama, erişim ve yetkilendirme sistem ve süreçlerinin oluşturulması ve izlenmesi.
- Denetim ve iç kontrol raporlarında yer alan tespitlere göre yapılacakların, gerçekleştirme tarihleriyle beraber bir aksiyon planına dönüştürülmesi ve üst yönetime onaylatılması.

Kurumsal SOME

- Bilgi güvenliği ihlallerine ilişkin gerçekleştirilen faaliyetlere yönelik yıllık olarak SOME Rehberinde belirtilen Kurumsal SOME Faaliyet Raporu düzenlenmesi, üst yönetime ve Birlik aracılığıyla Kurula iletilmesi.

İç Denetim

- Bilgi sistemleri denetim planı hazırlanması ve Yönetim Kurulu onayına sunulması.
- İlgili plan çerçevesinde yılda en az bir kez olacak şekilde bilgi sistemleri denetim çalışmalarının gerçekleştirilmesi, sonuçların Yönetim Kurulu'na raporlanması.
- İç denetim, bağımsız dış denetim ve sızma testi sonuçlarına göre planlanan aksiyonların takibi ve Şirket Yönetim Kurulu'na raporlanması.

İç Kontrol

- Bilgi sistemlerine yönelik yıllık iç kontrol programı hazırlanması ve Yönetim Kurulu onayına sunulması.
- İlgili program çerçevesinde periyodik kontrol faaliyetleri gerçekleştirilmesi, Yönetim Kurulu'na ve İç Denetim Birimi'ne raporlanması.
- İç kontrol bulgularının ve planlanan aksiyonların takibi ve raporlanması.

Tüm Kullanıcılar

- Görev ve faaliyetlerin, Bilgi Güvenliği Politikası, Bilgi Güvenliği Taahhütnamesi, ilgili diğer politika ve prosedürlere uygun yerine getirilmesi.
- İlgili politika ve prosedürlerle ilgili oluşabilecek her türlü uyumsuzluğun Bilgi Güvenliği Sorumlusuna iletilmesi.
- Bilginin alınması, depolanması, iletilmesi, işlenmesi amaçlarıyla kullanılan yazılım, donanım, araç ve gereçlerden oluşan bilgi teknolojileri kaynakları ile Şirket'e ait varlıkların korunması, kullanım amaç ve kurallarına uygun hareket edilmesi.
- Görevi gereği edindiği kişisel ve ticari verilerin gizliliğinin sağlanması, ilgili verilere yalnızca görev, yetki ve sorumluluk sınırları çerçevesinde erişim sağlanması, Şirket politika ve prosedürleri ile ilgili yasal mevzuata uygun olarak korunması.

5. POLİTİKA

Şirket, kurumun güvenirliğinin ve itibarının korunmasının, temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesinin, personel, müşteriler ve üçüncü taraflarla yapılan sözleşme şartlarına ve tabi olunan yasal düzenlemelere uygunluğun sağlanması amacıyla; Şirket varlıklarına yetkisiz erişimin engellenmesini, bilginin ve bilgi varlıklarının tam, eksiksiz ve doğru olmasını ve yetkili kullanıcıların ihtiyaç duydukları veriye ihtiyaç duydukları zaman erişebilmesini hedefler.

Bilgi güvenliği, Şirket'in bilgi varlıklarının aşağıdaki özelliklerinin korunmasıdır:

- **Gizlilik:** Bilgi sistemlerine ve bilgiye sadece yetkili kullanıcı, uygulama veya sistem tarafından erişilebilmesi.
- **Bütünlük:** Bilginin doğruluğun ve tamlığının korunması; bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunması.
- **Erişilebilirlik:** Bilginin yetkili kullanıcı, uygulama veya sistem tarafından talep edildiğinde erişilebilir ve kullanılabilir olması.

Bilgi güvenliği, sadece bilginin gizliliğinin değil, bütünlüğünün ve kullanılabilirliğinin de sağlanması ile mümkündür. Bilginin gizlilik gerekliliği, sadece yetkilendirme dâhilinde, gereken bilgi varlıklarına erişim verilmesi anlamına gelir. Bilginin bütünlüğü, tüm bilgi varlıklarının tamlığını ve doğruluğunu sağlamayı gerektirir. Bilginin kullanılabilirliği, bilgi varlıklarının ihtiyaç duyulduğu anda ulaşılabilir ve kullanılabilir olmasını gerektirir.

Şirket'in bilgi sistemleri yönetimi, Bilgi Güvenliği Politikası ve bağlı diğer politika, prosedür ve talimatlarla tanımlanmış esaslar ve sorumluluklar doğrultusunda planlanır, uygulanır, izlenir ve sürekli iyileştirilir.

Şirket bünyesinde bilgi güvenliğinin sağlanmasında nihai sorumluluk Yönetim Kuruluna aittir. Bu sorumluluk kapsamında Yönetim Kurulu tarafından, Şirket genelinde uygulanmasını gözetmekle yükümlü olduğu bir bilgi güvenliği yönetim sistemi tesis edilmiştir. Bilgi güvenliği yönetim sistemi aşağıdaki faaliyetleri içerir:

a) Bilgi sistemlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını,
b) Bilgi varlıklarının sınıflandırılarak varlık sahipliklerinin belirlenmesi ve varlık sınıflarına uygun güvenlik önlemlerinin alınması,
c) Bilgi güvenliği ihlallerinin takip edilmesi ve yılda en az bir kez değerlendirilmesi,
d) Şirket genelinde verilen hizmetlerde, görevler ayrılığı prensibi ile tutarlı etkin bir kimlik doğrulama ve erişim yönetimi tesis edilmesinin sağlanması,
e) Bilgi güvenliğinin sağlanmasına ilişkin kontrollerin ve tesis edilen yapıların test edilmesi ve test sonuçlarının takip edilerek raporlanması,
f) Bilgi varlıklarına yönelik güncel güvenlik açıklarının takip edilmesi ve gerekli aksiyonların alınmasının sağlanması,

g) Personele bilgi güvenliği gereksinimleri, riskler ve güncel tehditler konusunda bilgi düzeyini artırmaya yönelik eğitimlerin rol ve sorumluluklarına uygun şekilde yılda en az bir kez verilmesi ve bilgi güvenliği farkındalığını artıracak çalışmaların yapılması,
h) İş sürekliliği yönetimi kapsamında bilgi güvenliğini ilgilendiren hususların yer almasının sağlanması, asgari olarak kritik iş süreçlerini ve faaliyetlerini destekleyen bilgi sistemlerinin sürekliliğini sağlamak üzere iş sürekliliği planının bir parçası olan bilgi sistemleri süreklilik planı hazırlanması,

Dış hizmet alımlarının yönetimi kapsamında bilgi güvenliğini ilgilendiren hususların yer almasının sağlanması. Bilgi sistemleri güvenliğine ilişkin kontrollerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetimi hususunda Üst Yönetime rapor veren, bilgi sistemleri iç kontrol, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde yeterli teknik bilgiye ve en az 5 yıl tecrübeye sahip bir bilgi güvenliği sorumlusu belirlenir. Bilgi güvenliği sorumlusunun, bilgi sistemleri yönetimine ilişkin gerekliliklerin yerine getirilmesi hususunda herhangi bir görevinin bulunmaması ve üst yönetime bağlı çalışması sağlanır.

5.1 BİLGİ SİSTEMLERİ RİSK YÖNETİMİ

Bilginin kullanımı, yerleşimi ve korunması ile ilgili ihtiyaçların karmaşıklığı ve çokluğu, kapsamlı ve geniş bilgi güvenliği süreçlerinin ve politikalarının tanımlanmasını gerektirmektedir. Bu nedenle belirlenen süreçler doğrultusunda bilgi güvenliği riskleri, bilgi varlığından sorumlu olan kişiler tarafından değerlendirilir, risklerin önceliği belirlenir ve gereken önlemler alınır.

Bilgi sistemlerine ilişkin riskleri ölçmek, izlemek, işlemek ve raporlamak üzere risk yönetimi süreci ve prosedürleri tesis edilir ve güncelliği sağlanır. Bilgi sistemlerine ilişkin risklerin yönetilmesinde asgari olarak aşağıdaki hususlar değerlendirmeye katılır:

a) Bilgi teknolojilerindeki hızlı gelişmeler sebebiyle rekabetçi ortamda gelişmelere uymamanın olumsuz sonuçları, gelişmelere uyma konusundaki zorluklar ve yasal mevzuatın değişebilmesi,
b) Bilgi sistemleri kullanımının öngörülemeyen hatalara ve hileli işlemlere zemin hazırlayabilmesi,
c) Bilgi sistemlerinde dış kaynak kullanımından dolayı dış kaynak hizmeti veren kuruluşlara bağımlılığın oluşabilmesi,
d) İş ve hizmetlerin önemli oranda bilgi sistemlerine bağlı hale gelmesi,
e) Bilgi sistemleri üzerinden gerçekleştirilen işlemlerin, verilerin ve denetim izlerine ilişkin tutulan kayıtların güvenliğinin sağlanmasının zorlaşması.

Risk analizi yılda en az bir defa gerçekleştirilir. Bilgi sistemlerinde meydana gelecek önemli değişikliklerde tekrarlanır. Risk analizinde tüm bilgi varlıkları değerlendirmeye alınır.

Risk yönetiminde asgari olarak aşağıdaki faaliyetler yerine getirilir:
a) Risk değerlendirme kriterlerinin belirlenmesi.
b) Risklerin analiz edilmesi ve risk seviyelerinin belirlenmesi.

c) Bilgi sistemleri stratejisine ve mevzuata aykırılık teşkil etmeyecek şekilde, iş ve bilgi güvenliği hedefleriyle uyumlu risk kabul kriterleri ile risk işleme seçeneklerinin belirlenmesi ve üst yönetime onaylatılması.
d) İyileştirici faaliyetlerin gerekli iş gücü, kaynak ve zaman bilgisiyle kayıt altına alınması.
e) İyileştirici faaliyetlerin ve risk analizinin üst yönetime onaylatılması.
f) İyileştirici faaliyetlerin takibi ve bir sonraki analizde ele alınması.

Risk analizi kapsamında aşağıdaki faaliyetler yerine getirilir:

a) Varlık envanterindeki bilgi varlıklarına ilişkin tehdit ve güvenlik açıklarının tespit edilmesi suretiyle risklerin belirlenmesi,
b) Tespit edilen tehditlere ve güvenlik açıklarına göre bilgi varlıklarının riske maruz kalma olasılıklarının belirlenmesi,
c) Risklerin gerçekleşmesi durumunda ilişkili bilgi varlığının gizliliği, bütünlüğü, erişilebilirliği gibi kriterlerine olan etkilerin belirlenmesi suretiyle ilgili bilgi varlığına yönelik etki hesaplaması yapılması,
d) Bilgi varlıklarını tehdit eden risklerin belirlenen olasılık ve etki değerlerine göre risk derecelendirmesinin yapılması,
e) Risk analizinde gerçekleştirilen çalışmaların bütününü temsil eden özet risk değerlendirme raporunun hazırlanarak Üst Yönetime sunulması.

Risk analizi sonuçlarına göre tespit edilen risklerin ilişkili olduğu bilgi varlıklarının değerine ve Şirket'in risk limitlerine uygun olacak şekilde risklere ilişkin aksiyonlar belirlenir. Risk aksiyonlarının belirlenmesi aşamasında, riskin ilgili olduğu iş biriminin temsilcileriyle beraber risk analizi sonucunda, riskin azaltılması, riskten kaçınma, riskin kabulü ve riskin transferi gibi yöntemlerle nasıl ele alınacağına karar verilir.

Her bir risk için belirlenen aksiyonlar risk aksiyon planına dönüştürülür. Alınacak aksiyonlar için yapılacak kaynak aktarımında ve aksiyonların tamamlanma tarihlerinin önceliklendirilmesinde, risk analizi aşamasında belirlenen risk dereceleri dikkate alınır. Aksiyon planının uygulanması sonucunda kalacak artık riskler için de alınacak aksiyonlar planlanır ve aksiyon planı güncellenir.

Risk analizleri sonucu hazırlanan güncel risk değerlendirme raporu ve güncel risk aksiyon planı birleştirilerek Şirket'in bilgi sistemleri risk envanteri oluşturulur. Yılda en az bir defa olmak üzere veya bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce risk analizleri tekrarlanır. Tekrarlanan risk analizi sonuçlarına göre risk aksiyon planı ve risk envanterinin güncellenmesi sağlanır.

Şirket bünyesinde gerçekleştirilen bilgi sistemleri iç kontrol ve iç denetim çalışmalarının sonuçlarının veya tespit edilen bulguların risk envanterine girdi teşkil etmesi sağlanır.

Bilgi sistemleri risk yönetimine ilişkin detaylara "**Bilgi Güvenliği Risk Yönetimi Politikası**"nda yer verilmiştir.

Bilgi sistemleri, bilgi güvenliği gereklerinin yerine getirilmesi hususunda herhangi bir görevi bulunmayan ve sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından en az yılda bir kez, Kurul düzenlemelerinde yer alan usul ve esaslara uygun olarak sızma testine tabi tutulur. Sızma testleri sonucu tespit edilen bulgular, bulguların önem derecelerini, birlikte oluşturabilecekleri

riskleri, tespit edildiği varlıkların değerini ve sızma testi raporlarında yer alan önerileri dikkate alınarak, Şirket Yönetim Kurulunca onaylanan ve bu bulguların en kısa sürede giderilmesini amaçlayan bir aksiyon planı çerçevesinde takip edilir. Sızma testleri sonucu ortaya çıkan tespitler ve planlanan aksiyonlar Yönetim Kurulu'nun talebi üzerine önem derecesine göre İç Denetim Planına dahil edilebilir. Sızma testi raporları, tamamlanmasını müteakip bir ay içinde ve her durumda en geç takip eden yılın 31 Ocak tarihine kadar Kurul'a gönderilir.

5.2 BİLGİ SİSTEMLERİ KONTROLLERİNİN TESİSİ VE YÖNETİLMESİ

Üst Yönetim, Politika kapsamında, bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetildiğinden emin olmak için, bilgi sistemlerinin güvenliğini sağlayacak önlemlere ilişkin kontrollerin geliştirilmesini, işletilmesini, güncelliğini sağlar ve gerekli yönetsel sorumlulukları, asgari olarak aşağıdaki hususlar dikkate alarak tanımlar:

a) Her kontrol süreci için süreç sahibinin, rollerin, faaliyetlerin ve sorumlulukların açık bir şekilde tanımlanması,
b) Süreçlerin performansının ölçülebilmesi için ölçüm kriterleri tanımlanması,
c) Süreçler ve kontroller hakkında ilgili personelin yeterli eğitim alması,
d) Kontrol süreçlerinin periyodik biçimde tanımlanması,
e) Her kontrol sürecinin hedef ve amaçlarının açıkça tanımlanmış olması ve performansının ölçülebilir olması.

Söz konusu hususlara **Bilgi Sistemleri İç Kontrol Prosedürü'nde** yer verilmiştir.

Bilgi sistemleri kontrollerine ilişkin etkinlik, yeterlilik ve uygunluk ile öngörülen risk ya da risklerin etkisini azaltmaya yönelik faaliyetler devamlı bir şekilde takip edilir ve değerlendirilir. Değerlendirme neticesinde tespit edilen önemli kontrol eksiklikleri yılda en az bir kez Üst Yönetime raporlanır ve gerekli önlemlerin alınması sağlanır.

Verilerin güvenliğini ve bütünlüğünü korumak, veri değişikliklerini önlemek ve veri bütünlüğünü sağlamak için gerekli süreç akışı ve sorumluluklar, **Veri Bütünlüğü Politikası**'nda düzenlenmiştir.

5.3 VARLIK YÖNETİMİ

Şirket, sahip olduğu bilgi varlıklarını ve bu varlıkların sorumlularını belirler, bu varlıkların envanterini oluşturur ve envanterin güncelliğini sağlar.

Taşınabilir cihaz ve ortamlar, içerdiği bilgilerin güvenlik sınıfına göre kaybolma, hırsızlık ve kopyalama gibi risklere karşı korunur. Güvenlik sınıfı yüksek bilgileri veya bu bilgilere erişim sağlayan yazılımları barındıran taşınabilir cihaz ve ortamlar izinsiz Şirket dışına çıkarılmaz.

Bilgi varlıklarının ve verilerin güvenlik sınıfı, asgari olarak varlıkların gizlilik, bütünlük ve erişilebilirlik gereksinimleri, kritikliği ve hassasiyeti dikkate alınarak belirlenir.

Kullanımdan kaldırılan donanımsal varlıklara güvenli silme veya imha işlemleri uygulanır ve kayıt altına alınır. Kullanımdan kaldırılan yazılım ve uygulamalara erişimler engellenir ve gerekirse bu yazılım ve uygulamalar arşivlenerek sistemden silinir.

Bilgi sistemleri kapsamında sunulan hizmetler için, hizmetin tanımı, kullanıcıları, sahibi, hizmet seviyesi taahhütleri ve bağımlılıklarına ilişkin bilgileri içeren hizmet envanteri oluşturulur ve güncelliği sağlanır.

Bilgi sistemleri kapsamındaki süreçler için, sürecin tanımı, sahibi, girdi ve çıktıları ve bağımlılıklarını içeren süreç envanterini oluşturur ve güncelliğini sağlar.

Varlık envanterinin hazırlanması ve sınıflandırılmasına ilişkin detaylara "**Varlık Yönetimi Prosedürü**"nde yer verilmiştir.

5.4 GÖREVLER AYRILIĞI İLKESİ

Bilgi sistemleri üzerinde hata, eksiklik veya kötüye kullanım risklerini azaltmak için görev ve sorumluluk alanları ayrılır.

Kritik işlemlerin tek bir personele veya dış kaynak hizmeti sunan kuruluşa bağımlı olmaması amacıyla gerekli kritik personel yedeklemesi yapılır.

Sistem, veri tabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde görevler ayrılığı prensibi uygulanır. Bu amaçla görevler ayrılığı matrisi oluşturulur ve en az yılda bir kez olmak üzere gözden geçirilir ve güncelliği sağlanır.

Görevlerin tam ve uygun şekilde ayrılmasının mümkün olmadığı durumlarda oluşabilecek hata, eksiklik veya kötüye kullanımı önlemeye ve tespit etmeye yönelik telafi edici kontroller tesis edilir.

Bilgi sistemlerinin etkin ve düzenli bir şekilde yönetilmesi, güvenliği, performansı ve uyumluluğunun sağlanması için gerekli olan görevler ayrılığı ilkesine ilişkin çerçeve **Bilgi Sistemleri Görevler Ayrılığı Politikası**'nda açıklanmıştır.

5.5 FİZİKSEL VE ÇEVRESEL GÜVENLİK

Kritik varlıklar ve bunları destekleyen birimler güvenli alanlarda tutulur. Fiziksel erişimin yalnızca yetkilendirilmiş kişilerce yapılmasını sağlamak amacıyla, güvenli alanlar gerekli giriş kontrolleriyle korunur. Bu alanlara sadece erişim yetkisi olan personel tarafından uygun giriş kontrol yönetimi (resepsiyon görevlisi, madeni kilit, manyetik kartlı kapı kilidi, vb.) kullanılarak giriş yapılması sağlanır.

3.taraflarla etkileşimin yoğun olduğu işlerin yapılması için, sadece görev için gereken erişim ve izin sınırları içinde bulunulması, güvenli alanlardan uzak kalınması ve yapılan işlerin kaydının tutulması sağlanır. Güvenli alanlara giren ziyaretçilere, alanlarda bulundukları süre boyunca eşik edilir. Çalışanlar, 3.taraflar ve ziyaretçiler için erişim ihtiyacının sona ermesi durumunda, erişim yetkileri kapatılır.

Güvenli alanlara erişim yetkileri düzenli olarak gözden geçirilir. Güvenli alanlara giriş ve çıkışlar gerekçelendirilir, yetkilendirilir, kaydedilir ve izlenir.

Kritik varlıkların yangın, sel, deprem, patlama, yağma ve diğer doğal ya da insan kaynaklı felaketlerden kaynaklanan hasarlarına karşı sigorta dahil gerekli fiziksel koruma önlemleri alınır. Yedekler ve felaket anında ulaşılması gereken kaynaklar, gerekli tedbirler alınarak felaketten etkilenmeyecek uzaklıktaki yerlerde bulundurulur. Yangın önleme, acil durumda müdahale, ilkyardım planları, back-up anahtarların kullanımı planlar dâhilinde dokümante edilir. Bu aktivitelerin organizasyonu için takım ve birey sorumlulukları belirlenir. Bu önlemlere ait planlar gerektiğinde polis veya itfaiye gibi kuruluşların kullanabileceği ortamlarda bulundurulur.

Fiziksel ve çevresel bilgi güvenliği esaslarının detayları **Fiziksel ve Çevresel Güvenlik Prosedürü**'nde tanımlanmıştır.

5.6 AĞ GÜVENLİĞİ

1) Ağların tehditlere karşı korunması ve ağları kullanan sistem, veri tabanı ve uygulamaların güvenliğinin sağlanması için kontroller tesis edilir ve etkin bir şekilde yönetilir. Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisi esas alınır.

2) Şirket, dış ağı ve iç ağı arasındaki trafiği kontrol altında tutmak için gerektiği şekilde konfigürasyonu yapılmış ve sürekli gözetim altında tutulan güvenlik duvarı çözümleri ile saldırıları tespit edebilecek ve önleyebilecek günün teknolojisine uygun sistemler kullanır. Söz konusu uygulamaların detaylarına "**Ağ Güvenliği Yönetimi Prosedürü**"nde yer verilmiştir.

3) İç ağdan gelebilecek tehditlerin etkisini azaltmak ve iç ağın farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçişi temin etmek üzere Şirket iç ağındaki her bir servise ilişkin trafiğin yalnızca kendisi için gerekli olan ağ segmentlerine ulaşmasını sağlayacak şekilde Şirket iç ağı alt bölümlere ayrılır. Farklı ağ segmentleri arasındaki veri trafiğinin güvenliği sağlanır. İç ağa sadece yetkilendirilmiş cihazların bağlanabilmesi sağlanır.

4) Hassas veya sır kapsamındaki verilere sahip sistemlerin özel iç ağda bulunması ve hiçbir şekilde doğrudan internetten erişilemiyor olması sağlanır. Özel iç ağdaki sistemlerle yalnızca vekil uygulamalar veya güvenlik duvarı cihazları üzerinden iletişim kurulur.

5) Ağ üzerinde kimlik ve erişim yönetimine yönelik kurulan etki alanı yönetimi sunucuları gibi yapıların Şirket'e özgü oluşturulmuş olması ve Şirket dışındaki başka bir etki alanı ya da benzerinin parçası olmaması esastır.

6) Kritik ağ segmentlerine yapılan bağlantılar düzenli olarak tespit edilerek bu bağlantıların her biri için gereksinim değerlendirmesi yapılır ve gereksiz bağlantıların sonlandırılması sağlanır.

7) Bilgi Güvenliği Sorumlusu tarafından onaylanmadıkça Şirket personeli ya da dış hizmet sağlayıcıları tarafından Şirket içi uygulama ve sistemlere, Şirket dışından uzaktan erişim gerçekleştirilmez. Uzaktan erişimin gerçekleştiği hallerde ise **"Uzaktan Erişim Politikası"** kapsamında çok bileşenli kimlik doğrulamaya dayanan güvenli bağlantı yöntemleri uygulanır, erişimlere ilişkin iz kayıtları tutulur, bağlantının süresi ve bağlantının yapılabileceği cihazlar kısıtlanır ve kullanıcı belli aralıklarla kimliğini

tekrar doğrulamaya zorlanır. Belirli konumlardan ve ekipmanlardan gelen bağlantıları yetkilendirmek için otomatik ekipman tanımlaması göz önüne alınır. Bu tür erişimlerin hem kullanılan sistemler hem de erişim yöntemleri açısından içerdiği riskleri en aza indirgeyecek önlemler oluşturulur.

8) İnternet üzerinden veya Şirket dış ağından görünür olan sunucu ve sistemler, görünür olmalarını gerektirecek geçerli bir iş ihtiyacı olup olmadığının tespit edilmesi amacıyla düzenli olarak kontrol edilir ve eğer gerekli değilse bu sunucu ve sistemlerin Şirket iç ağına taşınması ve iç ağ IP adreslerine sahip olması sağlanır.

9) Şirket, iç ağından dış ağa akan trafik içeriğini kontrol eder. Yapılacak içerik kontrolünün, zararlı IP adreslerine olan trafik akışını ve hassas veriler ile sır kapsamındaki verilerin sızdırılmasını engelleyecek nitelikte olması ve oturum bilgilerini kayıt altına alarak olağan dışı uzun süreli oturumları tespit edecek ve bunlar için uyarı üretebilecek yetenekte olması sağlanır.

10) Şirket'ten gönderilen e-postalar için e-posta sunucularında gönderici kimliğini doğrulayıcı teknikler kullanılır.

11) İletişim altyapıları dinlemeye ve fiziksel hasarlara karşı korunur.

12) Bilgi sistemleri altyapısına yönelik yetkisiz erişimler engellenir ve denetim izleri tutularak gözetim süreçleri tesis edilir.

13) İç kaynak yoluyla sağlanan veya dış kaynak kullanımı yoluyla alınan her türlü ağ hizmetinin güvenlik kriterleri, hizmet düzeyleri ve yönetim gereksinimleri tanımlanır ve hizmet anlaşmalarına dâhil edilir.

5.7 GÜVENLİK KONFİGÜRASYONU YÖNETİMİ

1) Şirket, masaüstü, dizüstü, mobil cihazlar ve sunucuları üzerindeki işletim sistemi, veri tabanları ve uygulamalar ile güvenlik duvarları, yönlendirici ve anahtarlama cihazları (firewall, ana router, DMZ, VPN switch vb.) kritik ağ bileşenleri için sıkılaştırılmış ve test edilmiş güvenli standart konfigürasyon bilgilerini oluşturur.

2) Bu standart konfigürasyon bilgileri, standart konfigürasyondan sapmalar veya standart konfigürasyondaki güncellemeler değişiklik yönetiminin bir parçası olarak kayıt altına alınır ve onay mekanizmasına tabi tutulur. Güvenli standart konfigürasyon dışında kalacak her türlü değişiklik isteği için bu değişikliği gerektiren iş gereksinimi ve bu iş gereksinimine ihtiyaç duyan iş sorumlusunun kim olduğu ve gereksinim süresi gibi bilgiler de kayıt altına alınır.

3) Şirket; masaüstü, dizüstü, mobil cihazlar ve sunucular üzerindeki işletim sistemleri için bu işletim sistemlerinin tipi, versiyon numarası, yama seviyesi ve üzerinde yüklü olan veri tabanları ve uygulamaların listesini gösterecek şekilde bir **yazılım envanteri** tutar. Kullanılacak yazılım envanterinin aynı zamanda **donanım envanteri** ile de entegre olması ve tek bir noktadan hangi donanım üzerinde hangi yazılımların olduğu bilgisinin takip edilebilir olması sağlanır.

4) Masaüstü ve dizüstü makineleri ile sunucuları, bu makinelere taşınabilir bir medya veya harici cihaz takıldığında otomatik olarak içeriği oynatmayacak şekilde yapılandırılır ve zararlı yazılım engelleme

araçları bu tür cihazlar takıldığında otomatik olarak bu cihazları tarayacak şekilde ayarlanır. Bunun yanında bu tür harici cihazların makinelere bağlanacağı bağlantı arayüzlerinin ön tanımlı olarak kullanıma kapatılarak bu tür cihazların kullanımının yalnızca iş gereksinimi olan kullanıcılarla sınırlı tutulması ve harici cihazları kullanma denemesi yapılan durumların da takip edilmesi sağlanır.

5) Mobil cihazların ağ erişimine ilişkin esaslar "**Mobil Cihaz Güvenliği Politikası"**nda belirlenmiştir.

6) Ağa bağlı her bir sistem üzerindeki portların, protokol ve servislerin sadece gerekliliği onaylanmış iş ihtiyaçlarına istinaden açık ve çalışıyor olması sağlanır. Bu doğrultuda, güvenli bir baz konfigürasyonu temel alınarak önemli sunucu ve sistemler için düzenli olarak port taraması gerçekleştirilir ve güvenli baz konfigürasyonda bulunmadığı halde açık durumda olan portların kapatılması sağlanır.

5.8 GÜVENLİK AÇIKLARI VE YAMA YÖNETİMİ

1) Şirket faaliyetlerini kesintiye uğratacak veya önemli ölçüde olumsuz etkileyecek durumların ortaya çıkma olasılığını azaltmak için sistem, yazılım ve cihazlardaki güvenlik açıklarını hızlı ve etkin bir şekilde ele alacak bir güvenlik açıkları ve yama yönetimi süreci tesis edilir. Güvenlik açıkları ve yama yönetimi süreci kapsamında gerçekleştirilen faaliyetler değişiklik yönetiminin bir parçası olarak kayıt altına alınır ve onay mekanizmasına tabi tutulur. Süreç kapsamındaki faaliyetlere **Yama Yönetimi Prosedürü'nde** yer verilmiştir.

2) Sağlayıcı veya üretici desteği biten sistem, yazılım ve cihazlar artık güncellenemediğinde, bunlar için yüklenebilen en son güncellemelerin günün şartlarına göre artık güvenli olmaması ve telafi edici kontroller ile de makul seviyede bir güvenlik sağlanamaması halinde sistem, yazılım ve cihazlar kullanımdan kaldırılır.

3) Şirket, ağa bağlı olan sistem ve cihazlarına yönelik olarak otomatik güvenlik açığı tarama araçları kullanır. Tespit edilen her bir güvenlik açığıyla ilgili olarak bilgi güvenliği sorumlusuna ve açığın tespit edildiği sistemden sorumlu sistem yöneticisine en kritik güvenlik açıklarını öncelikli olarak listeleyecek şekilde raporlama yapılır.

4) Masaüstü ve dizüstü makineleri ile sunucuları, sürekli bir şekilde izlenerek üzerindeki zararlı yazılımların tespit edilmesi sağlanır.

5) E-posta sunucusuna gelen ve giden e-postalar taranarak zararlı yazılım barındıran ya da Şirket'in iş ihtiyaçları doğrultusunda gereksiz olan eklentiler içeren e-postaları engelleyecek çözümler kullanılır. Şirket e-postalarının kişisel ve iş amaçlı kullanımına yönelik olarak kurallar ve esaslar **E-Posta Politikası**'nda tanımlanmıştır.

5.9 ZARARLI YAZILIMLARDAN KORUNMA

Şirket bünyesinde kullanılacak yazılımların ve verinin işlerliğini ve bütünlüğünü koruyacak tedbirler alınır ve bu durumların tespitine yönelik mekanizmalar kullanılır.

Bilgisayar virüsleri, solucanları, Truva atları, casus yazılımlar, arka kapılar, klavye dinleme sistemleri ve mesaj sağanakları (spam) gibi zararlı yazılımların (malware); mobil veya yerleşik bilgi işleme imkânlarına

bulaşması, yayılması ve zarar vermesi, kendiliğinden devreye giren ve sık sık güncellenen güçlü zararlı yazılım önleyici yazılımlar ile engellenir.

Sistemlere yüklenen programların lisanslı olması ve güvenilir kaynaklardan temin edilmesi sağlanır. Dışarıdan transfer edilen veya güvenilmeyen bir erişim üzerinden edinilen her türlü yazılım ve veri taramadan geçirilir.

Sistemlerde istem dışı oluşan değişikliklerin tespiti için, bunları tespit eden yazılımlar kullanılır. Sistemlerde, bilgi dâhilinde olmaksızın oluşan, dosyaların ve değişikliklerin nedenleri araştırılır.

Zararlı yazılımların temizlenmesi belirli bir prosedür dâhilinde yapılır. Temizlik esnasında çalışan yapıya zarar verilmemesi esastır.

Tüm kullanıcılar virüs ve benzeri türdeki yazılımlar ve bunların etkileri hakkında bilgilendirilir. Zararlı yazılımlara karşı tedbir almanın, bu yazılımların etkilerini ortadan kaldırmaktan daha kolay ve etkin bir çözüm olduğu bilinci oluşturulur. Tüm kullanıcılar virüslere karşı duyurulan önlemleri almak ve bunlara uymakla yükümlüdürler.

Zararlı yazılımlara ilişkin tedbirlere **Antivirüs Kullanım Politikası'nda** yer verilmiştir.

5.10 KİMLİK DOĞRULAMA

Bilgi sistemleri üzerinden gerçekleşen işlemler için, risk değerlendirmesi sonucuna uygun kimlik doğrulama yöntemi belirlenir. Yöntem tercih edilirken, bilgi sistemleri üzerinden gerçekleştirilmesi planlanan işlemlerin niteliği, doğurabileceği finansal veya finansal olmayan etkilerinin büyüklüğü, işleme konu verinin, hassasiyeti ve kimlik doğrulama yönteminin kullanım kolaylığı göz önünde bulundurulur.

Kimlik doğrulama yöntemi, müşterilerin ve personelin bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek tüm süreci kapsayacak şekilde uygulanır. Kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek gerekli önlemler alınır.

Parola kullanımı gerektiren kimlik doğrulama yöntemlerinde, parolaların tahmin edilmesi ve kırılması zor bir karmaşıklıkta ve uzunlukta olması sağlanır. Kullanıcılara ilk kez verilen ya da unutulması durumunda iletilen geçici şifreler derhal kullanıcı tarafından değiştirilir. Geçici şifrelerin kullanıcıya güvenli bir şekilde iletilmesi ve kullanıcının geçici şifresini değiştirip farklı bir şifre ile erişimlerini yapabildiğine dair teyidi dönmesi sağlanır. Şifreler belirli aralıklarla değiştirilir. Şifreler sistemlerde okunamayacakları kriptolu olarak ve güvenli bir ortamda tutulur. Parola kullanımına ilişkin detaylar "**Parola Politikası"**nda düzenlenmiştir.

Kullanılan kimlik doğrulama verilerinin tutulduğu ortamların ve bu amaçla kullanılan araçların güvenliğini sağlamaya yönelik gerekli önlemler alınır. Bu önlemler asgari olarak kimlik doğrulama verilerinin şifreli olarak saklanması, bu veriler üzerinde yapılacak her türlü değişikliği algılayacak sistemlerin kurulması, yeterli denetim izlerinin tutulması ve güvenliğinin sağlanması hususlarını içerir. Kimlik doğrulama verilerinin aktarımı sırasında gizliliğinin sağlanmasına yönelik önlemler alınır.

5.11 ERİŞİM YÖNETİMİ

Bilgi sistemlerine erişim **Kimlik ve Erişim Yönetimi Politikası** çerçevesinde sağlanır.

Yetkilendirme düzeyi ve erişim haklarının atanmasında görev ve sorumluluklar göz önünde bulundurularak, gerekli olacak en düşük yetkinin atanması ve en kısıtlı erişim hakkının verilmesi yaklaşımı esas alınır. Atanacak yetkiler ve sorumluluklar görevler ayrılığı ilkesi ile tutarlı olur.

Bilgilere, servislere ve verilere erişim hakları, işin sahibi tarafından belirlenip dokümante edilir ve Bilgi Güvenliği Sorumlusuna iletilir.

Tüm yetkiler ve erişim hakları her yıl güncel durumla uyumlulukları açısından değerlendirilmeye tabi tutulur. Kullanıcılara tanımlanan erişimler, düzenli erişimler için en az altı ayda bir, istisnai erişimler için en az üç ayda bir onay veren birim tarafından gözden geçirilir.

Yetkilendirme verilerinin güvenliği sağlanır ve bu veriler üzerinde yapılacak her türlü değişikliği algılayacak kayıt sistemleri kurulur. Yetkilendirme verilerinin tutulduğu ortamlara yetkisiz erişim teşebbüsleri kayıt altına alınır ve düzenli olarak gözden geçirilir.

Ayrılan veya sistem erişimine ihtiyacı kalmayan kullanıcının erişimleri ivedilikle kaldırılır.

İstisnai (sistem ve kaynaklarda önemli alanları etkileyebilecek erişimler, sistem ve kullanıcı yönetimine ait erişimler veya ürünlerin yönetimi için gereken erişimler...) erişim talepleri, prosedüre göre ve onaylaması halinde yapılır. Bu tür erişimlerin gerekliliği ve seviyelendirilmesi sistem ve ürün başına ayrı ayrı yapılır. Sadece gerektiği ölçüde, gerekli süre içinde gerekli amaç için yeterli olacak kadar erişim tanımlanır. Verilen erişimlerin kaydı tutulur ve bu erişimlerin tanımlanması veya değiştirilmesi gibi durumlar takip edilir. Bu tür istisnai erişimler için normal erişimde kullanılandan farklı bir kullanıcı kodu tanımlanır.

Bilişim kaynaklarına izinsiz erişimleri önlemek için kullanıcıların katılımına yönelik bilincin ve tedbirlerin oluşturulması sağlanır.

5.12 İŞLEMLERİN, KAYITLARIN VE VERİLERİN BÜTÜNLÜĞÜ

Bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli önlemleri alır. Bütünlüğü sağlamaya yönelik önlemler verinin iletimi, işlenmesi ve saklanması aşamalarının tamamını kapsayacak şekilde tesis edilir.

Bilgi sistemlerine ilişkin dış kaynak hizmeti alınan kuruluşlar nezdinde gerçekleşen işlemler için de aynı yaklaşım gösterilir.

Kritik işlemler, kayıtlar ve verilerde meydana gelebilecek bozulmaları saptayacak teknikler kullanılır.

5.13 VERİLERİN GİZLİLİĞİ

Şirket faaliyetleri kapsamında gerçekleşen işlemlerin ve bu işlemler kapsamında iletilen, işlenen ve saklanan verilerin gizliliğini sağlamaya ve önem derecesi yüksek verilerin kasten veya yanlışlıkla kurum dışına sızmasını önlemeye yönelik tedbirler alınır.

Verilerin tutulduğu ortamın kâğıt veya elektronik ortam olmasından bağımsız olarak alınacak önlemlerin, gizliliği sağlanmaya çalışılan verilerin önem derecesine uygun olması ve gerekli yerlerde ek kontrollerin tesis edilmesi esastır.

Verilere erişim haklarının kişilerin görev ve sorumlulukları çerçevesinde belirlenmesi, erişimlerin kayıt altına alınması, bu kayıtların yetkisiz erişim ve müdahalelere karşı korunması sağlanır.

Veri gizliliğini sağlamada kullanılacak şifreleme teknikleri için güncel durum itibarıyla güvenilirliğini yitirmemiş ve günün teknolojisine uygun algoritmalar kullanılır. Kullanılacak şifreleme anahtarları, ilgili algoritmalar için anahtarın geçerli olacağı ve kullanılabileceği zaman zarfında kırılamayacak şekilde uzun seçilir ve ilgili veri ya da operasyonun kritiklik seviyesine göre bu anahtarların geçerlilik süresi belirlenir. Geçerlilik süresi dolan ya da güvenilirliğini yitirdiği tespit edilen şifreleme anahtarlarının kullanımı derhal engellenir. Şifreleme anahtarlarının yaşam döngüsü boyunca güvenliğinin sağlanması, güvenli bir şekilde oluşturulması, müşteri ve personel kullanımına sunulması ve saklanması esastır. Verilerin gerektirdiği güvenlik düzeyine uygun olarak şifrelenerek saklanması, şifrelemede kullanılan anahtarların yönetim, güvenliğinin sağlanması ve verilerin güvenli iletimi için kullanılacak yöntemlerle bunların kullanım biçimleri **Veri Şifreleme ve Anahtar Yönetimi Prosedürü'**nde düzenlenmiştir.

Hassas verilerin farklı güvenlik seviyesine sahip ortamlar arasında iletiminde uçtan uca güvenli iletişimin kullanılması ve bu verilerin şifrelenmiş bir şekilde saklanması esastır. Şirket'in personeline tahsis ettiği hassas veya sır kapsamındaki veri içeren masaüstü, dizüstü ve mobil cihazların içeriğinin şifrelenmesi sağlanır ve ağa bağlı sunucu cihazlar üzerinde açık metin halinde hassas verilerin bulunup bulunmadığını belirlemek için sunucu makineleri taranır.

Veri barındıran medya ya da cihazların kullanımdan kaldırılması durumunda, içerdikleri verilerin gizlilik derecesine uygun olarak güvenli bir şekilde imha edilmesi sağlanır. İmha sürecine ilişkin detaylara **"Veri İmha Politikası"** nda yer verilmiştir.

5.14 MÜŞTERİ BİLGİLERİNİN GİZLİLİĞİ

Şirket, müşterinin kendisinden gelen ve yazılı şekilde ya da kalıcı veri saklayıcısı yoluyla kanıtlanabilir nitelikte olan bir müşteri talebi olmaksızın, faaliyetlerinin ifası sırasında ve her türlü dış hizmet alımlarında bilgi sistemleri aracılığıyla edindiği, sakladığı veya işlediği müşteri sırrı niteliğindeki bilgileri, yasalarda yer alan istisnai haller haricinde yurtiçindeki ve yurtdışındaki üçüncü kişilerle paylaşamaz ve bunlara aktaramaz.

Müşterinin, bilgilerini paylaşmaya dair açık rıza göstermesi verilecek hizmet için bir ön şart haline getirilemez.

Şirket, bilgi sistemleri aracılığıyla edindiği veya sakladığı müşteri bilgilerinin gizliliğini sağlanmasına; personel tarafından kişisel verilerin korunması ve işlenmesine yönelik kontrolleri tesis eder ve bunların gerektirdiği önlemleri alır. Söz konusu tedbirlere "Kişisel Verilerin Korunması ve İşlenmesi Politikası"nda yer verilmiştir.

5.15 ÜÇÜNCÜ TARAFLARLA BİLGİ DEĞİŞİMİ

Üçüncü taraflara Şirket bilgi sistemine erişim hakkı verilmeden önce gerekli güvenlik gereksinimleri tanımlanır ve uygulanır. Şirket'in bilgi içeren ortamları, üçüncü taraflar ile yapılan veri aktarımları sırasında gerçekleşebilecek kötüye kullanım veya bozulmaya karşı korunur. Bu kapsamda yapılan çalışmalar yazılı hale getirilir ve veri aktarımlarına ilişkin denetim izi tutulur.

Veri paylaşımına ilişkin detaylara **Kişisel Verilerin Korunması ve İşlenmesi Politikası**"nda yer verilmiştir.

5.16 MÜŞTERİLERİN BİLGİLENDİRİLMESİ

Şirket tarafından elektronik ortamda sunulan hizmetlerden yararlanacak müşteriler, sunulan hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak Şirket web sitesi ve ilgili sözleşme ve formlar vasıtasıyla açık bir şekilde bilgilendirilir ve söz konusu hizmetlere ilişkin risklerin etkisini azaltmaya yönelik olarak benimsenen bilgi güvenliği ilkeleri ve bu risklerden korunmak için kullanılması gereken yöntemler ilgili kanallarda müşterilerin dikkatine sunulur.

Bilgi sistemlerinden ve bunlara dayalı olarak verilen hizmetlerden dolayı müşterilerin yaşayabileceği sorunlar **Şikâyet Yönetimi Politikası** doğrultusunda ele alınır. Müşterilerin şikâyetlerini ulaştırmalarına imkân tanıyacak mekanizmalar oluşturulur ve Şirket web sitesinde duyurulur. **Şikâyet Yönetimi Politikası** kapsamında alınan şikâyet ve talepler değerlendirilerek aksaklıkları gidermeye ve müşteri memnuniyeti sağlamaya yönelik çalışmalar yapılır.

5.17 BİLGİ SİSTEMLERİNE İLİŞKİN DIŞARIDAN ALINAN HİZMETLERİN YÖNETİMİ

Üst Yönetim tarafından, bilgi sistemleri kapsamında dış kaynak yoluyla alınacak hizmetlerin doğuracağı risklerin yeterli düzeyde değerlendirilmesine, yönetilmesine ve dış kaynak yoluyla alınan hizmeti sağlayan kuruluşlarla ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayacak, asgari olarak aşağıdaki hususları içeren bir gözetim mekanizması tesis edilir:

Dış kaynak yoluyla alınan bilgi sistemleri hizmeti kapsamındaki tüm sistem ve süreçlerin Şirket risk yönetimi, güvenlik, gizlilik ve müşteri gizliliğine ilişkin ilkelerine uygun olması,

a) Şirket verilerinin dış kaynak yoluyla alınan bilgi sistemleri hizmeti sağlayan kuruluşa aktarılmasının gerekli olduğu durumlarda, söz konusu kuruluşun bilgi güvenliği konusundaki ilke ve uygulamalarının en az Şirket'in uyguladığı düzeyde olması,
b) Dış kaynak yoluyla alınan bilgi sistemleri hizmetine ilişkin hususların Şirket iş sürekliliği göz önünde bulundurularak düzenlenmesi ve gerekli önlemlerin alınması,
c) Dış kaynak yoluyla alınan bilgi sistemleri hizmetlerinde ölçme, değerlendirme, raporlama ve güvenlik fonksiyonlarında nihai sorumluluğun Şirket'te olması,
d) Dış kaynak yoluyla alınan hizmetin, Şirket'in yasal yükümlülüklerini yerine getirmelerini ve etkin biçimde denetlenmelerini engelleyici nitelikte olmaması,
e) Şirket'in önem arz eden konulara ilişkin dış kaynak hizmeti aldığı kuruluşlarla sözleşme imzalamadan önce ilgili kuruluş bünyesinde dış kaynak hizmetini istenilen kalitede gerçekleştirebilecek düzeyde teknik donanım ve altyapı, mali güç, tecrübe, bilgi birikimi ve insan

kaynağı bulunup bulunmadığı hususlarını da dikkate alacak şekilde inceleme ve değerlendirme çalışması yapmaları ve bu çalışma sonucunda hazırlanacak teknik yeterlilik raporunun Üst Yönetime sunulması.

Dış kaynak kullanımına ilişkin koşul, kapsam ve her türlü diğer tanımlama, dış kaynak yoluyla alınan hizmeti sağlayan kuruluşça da imzalanmış olacak şekilde sözleşmeye bağlanır. Sözleşme, asgari olarak Tebliğ'in 18/2 maddesinde belirtilen hususları içerir.

Dış kaynak yoluyla alınan hizmeti sağlayan kuruluşlara verilen erişim hakları özel olarak değerlendirilir. Fiziksel veya mantıksal olabilecek bu erişimler için risk değerlendirmesi yapılır, gerekiyorsa ek kontroller tesis edilir. Risk değerlendirmesi yapılırken ihtiyaç duyulan erişim türü, erişilecek verinin önemi ile erişimin bilgi güvenliği üzerindeki etkileri dikkate alınır. Alınan hizmetin sonlanması durumunda ilgili tüm erişim hakları iptal edilir.

Dış kaynak yoluyla gerçekleştirilen hizmetler için hizmetin erişilebilirliği, performansı, kalitesi, bu hizmet kapsamında gerçekleşen güvenlik ihlali olayları ile dış kaynak yoluyla hizmet sağlayan kuruluşun güvenlik kontrolleri, finansal koşulları ve sözleşmeye uygunluğu Bilgi Güvenliği Sorumlusu tarafından ilgili iş birimi yöneticileri ile koordineli olarak gerçekleştirilir.

Detaylara **Bilgi Sistemleri Dış Kaynak Yönetimi Prosedürü**'nde yer verilmiştir.

5.18 KAYIT MEKANİZMASININ OLUŞTURULMASI

Şirket, bilgi sistemleri üzerindeki riskleri, sistem veya faaliyetlerin karmaşıklığını ve kapsamının genişliğini göz önünde bulundurarak bilgi sistemlerinin kullanımına ilişkin etkin bir denetim izi (log) kayıt mekanizması tesis ederek bilgi sistemleri dâhilinde gerçekleşen faaliyetlere ait kayıtlarda değişiklik ve silmeye sebep olan işlemlere ilişkin denetim izlerinin yeterli detayda ve açıklıkta kaydedilmesi sağlar.

Kayıt mekanizmasının yetkisiz sistemsel ve kullanıcı erişimlerine karşı korunmasına yönelik önlemler alınır.

Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılır. Denetim izlerinin bütünlüğü düzenli olarak gözden geçirilir ve olağandışı durumlar Üst Yönetime raporlanır.

Denetim izlerinde asgari olarak aşağıdaki bilgiler tutulur:

a) Yapılan işlemlerin türü ve niteliği,
b) İşlemlere ilişkin yetkisiz erişim teşebbüsleri,
c) İşlemi gerçekleştiren uygulama,
d) İşlemi gerçekleştiren kişinin kimliği,
e) Yapılan işlemlerin zamanı.

Denetim izleri asgari 5 yıl saklanır. Denetim izlerinin, yeterli güvenlik düzeyine sahip ortamlarda korunması ve yedeklerinin alınması suretiyle, yaşanması muhtemel olumsuzluklar sonrasında da öngörülen süre için erişilebilir olmaları temin edilir.

Dış kaynak hizmeti alınan kuruluşlar, müşteriler ve personel, bilgi sistemleri üzerindeki aktivitelerinin kaydının tutulduğu konusunda bilgilendirilir. Denetim izlerinin tutulması Şirket'in belge saklamasına ilişkin yasal düzenlemelerden kaynaklanan yükümlülüklerini değiştirmez.

Log kayıtları konusunda hem tutarlılık sağlayabilmek hem de gerektiğinde sorunun kaynağını belirlemek için bilgi sistemlerinde kullanılan zaman bilgisi tek bir referans kaynağına göre senkronize edilir. Zaman bilgisi atomik saatler vasıtasıyla temin edilir.

Detaylara "**Denetim İzleri Yönetimi Prosedürü**"nde yer verilmiştir.

5.19 ZAMAN SENKRONİZASYONU

Zaman senkronizasyonu, tüm sistem bileşenlerinin aynı zaman dilimini paylaşmasını ve doğru saat ve tarih bilgilerini kullanmasını sağlar. Şirket'in bilgi sistemlerinde kullandığı zaman bilgisi tek bir referans kaynağına göre senkronize edilir. Zaman bilgisi atomik saatler vasıtasıyla temin edilir. Sürecin detayları **Zaman Senkronizasyonu Prosedürü**'nde düzenlenmiştir.

Bu, iş süreçlerinin düzgün çalışmasını, güvenlik önlemlerinin etkili olmasını ve verilerin düzgün bir şekilde izlenmesini sağlar

5.20 BİLGİ GÜVENLİĞİ İHLALİ

Şirket bünyesinde gerçekleşen her türlü bilgi güvenliği ihlal olayının ve bilgi sistemlerine ilişkin ortaya çıkan zayıflıkların yönetilmesini sağlayacak kontroller asgari olarak aşağıdaki hususları içerecek şekilde "**Bilgi Güvenliği İhlal Yönetimi Prosedürü**"nde düzenlenmiştir.

Gerçekleşen ihlal veya ortaya çıkan zayıflığın mümkün olan en kısa sürede kayda alınması ve çözülmesi için gerekli mekanizmaların kurulması, sorumlulukların belirlenmesi ve tüm personelin bilgilendirilmesi,

a) İhlal olayını veya zayıflığı bildiren kişinin, işlemin sonucu hakkında bilgilendirilmesi,
b) Bildirimi yapılan tüm ihlal olayı ve zayıflıkların kök sebebinin bulunması ve düzeltici faaliyetlerin uygulanması,
c) Kritik ihlal olayları veya zayıflıkların Üst Yönetime raporlanması,
d) Tüm ihlal ve zayıflıkların; türü, ortaya çıkış zamanı, etkilediği bilgi sistemleri, iş süreçleri ve etki alanı ile buna karşı gerçekleştirilen düzeltici faaliyetler, harcanan zaman, maliyet ve işgücü miktarının kayda alınması,
e) Tekrarlayan veya benzer ihlal veya zayıflıklara organizasyonun hazırlıklı olmasının sağlanması

Bilgi güvenliğini etkileyen kötü niyetli olaylar, erişim ihlâlleri, çevresel hasarlar, bilgi varlıklarının uygunsuz kullanım örnekleri, bilgi varlıklarına yönelik hırsızlık ve kayıp olayları, elektronik iletişim ortamında olağan dışı tarzda muhatap olunma ve diğer sosyal mühendislik olayları ve benzeri şüpheli durumlar ile karşılaşılır karşılaşılmaz, **Bilgi Güvenliği İhlal Yönetimi Prosedürü** doğrultusunda ilgili birim ve sorumlulara derhal haber verilmesi sağlanır. Bilgi Güvenliği Politikasını ihlal ederek bu tür sorunlara ve aksaklıklara neden olduğu tespit edilen kişiler için, **Disiplin Prosedürü** hükümleri uygulanır.

Şirket bünyesinde Kurumsal SOME kurulur ve SOME Tebliğinde belirtilen usul ve esaslara göre çalışır. Kurumsal SOME üyelerinin iletişim bilgileri USOM tarafından belirlenen yöntem ile USOM'a bildirilir ve güncelliği sağlanır. Bilgi güvenliği ihlallerine ilişkin gerçekleştirilen faaliyetlere yönelik yıllık olarak SOME Rehberinde belirtilen Kurumsal SOME Faaliyet Raporu düzenlenir, üst yönetime raporlanır. Hazırlanan rapor takip eden yıl 31 Ocak tarihine kadar Birlik aracılığıyla Kurula iletilir. Raporda, Kurumsal SOME Rehberinde belirtilenlerin yanı sıra asgari olarak aşağıdaki unsurlara da yer verilir:

a) Yaşanan olaylara cevaben yapılan tüm müdahaleler.
b) Otomatik yollarla tespit edilen ve yanıtlanan olayların sayısı ve türleri.
c) Bir tehdit aktörünün bilgi sistemleri ortamında bulunduğu süre (bir saldırganın tespit edildiği andan itibaren varlığının en erken kanıtına kadar geçen süre).
d) Kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybı performans metrikleri açısından değerlendirmeler.

5.21 BİLGİ SİSTEMLERİ EDİNİMİ, GELİŞTİRİLMESİ VE BAKIMI

Şirket, bilgi sistemleri edinimi, geliştirilmesi ve bakımı için asgari olarak aşağıdaki hususları içeren kontrolleri tesis eder:

a) Şirket'in kendi bünyesinde geliştirilecek, değiştirilecek veya dış kaynak hizmeti yoluyla edinilecek her türlü bilgi sisteminin, fonksiyonel gereksinimleri ile tasarım, geliştirme ve test aşamalarının her biri için teknik ve güvenlik gereksinimleri, planlama, test ve uygulama adımları **Uygulama Geliştirme Prosedürü**'nde detaylı olarak ele alınır.

b) Temin edilecek bilgi sistemleri yapısının Şirket'in ölçeği, faaliyetlerinin ve sunulan ürünlerin niteliği ve karmaşıklığı ile uyumlu olması sağlanır.

c) Yürütülecek bilgi sistemleri projelerinin doğru önceliklendirilmesini ve koordinasyonunu sağlamak ve bu projeler yoluyla edinilecek ya da geliştirilecek bilgi sistemlerinin, zamanında ve gerekli işlevsellik düzeyine sahip olacak şekilde teslim edilmesini sağlamak üzere **Proje Yönetimi Prosedürü** doğrultusunda bir proje yönetim süreci uygulanır. Proje yönetim süreci, projelerin büyüklüklerine, karmaşıklıklarına ve risklilikliklerine göre uygun bir yönetim yapısı tesis edilmesini sağlar.

d) Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projeler **Proje Yönetimi Prosedürü** çerçevesinde yapılan proje risk analizi sonucu belirlenir. Kritik projeler Üst yönetim tarafından gözden geçirilir ve bunlara ilişkin risklerin yönetilebilirliği göz önünde bulundurularak onaylanır. Kritik projelerin Şirket'in iç kaynaklarıyla veya dış kaynak yoluyla alınan hizmetlerle gerçekleştirilmesine bakılmaksızın personel uzmanlığının, projelerin teknik gereksinimlerini karşılayabilecek nitelikte olması esastır. Bu yapıyı desteklemek üzere oluşturulacak yönetsel rol ve sorumluluklar Üst Yönetim tarafından açıkça belirlenir.

e) Bilgi sistemlerinin geliştirme, değişiklik veya edinimi faaliyeti boyunca, işin gelişimini takip edebilmek için proje gelişim raporları hazırlanır ve Şirket'in Yönetim Kurulu tarafından onaylanır.

f) Uygulamalarda veri girişlerinin tam, doğru ve geçerli şekilde yapılmasını, veri üzerindeki işlemlerin doğru sonuçları üretmesini sağlayacak, veri ve işlem kaybını, verinin yetkisiz değiştirilmesini ve kötüye kullanımını önleyecek uygun kontroller tesis edilir.

g) Uygulama güvenliği ve erişilebilirlik gereksinimleri belirlenirken Şirket'in belirlemiş olduğu veri sınıflandırması ve risk öncelikleri göz önünde bulundurulur.

h) Bilgi sistemleri gerçek ortamda kullanıma alınmadan önce kabul kriterleri belirlenir, hazırlanacak bir plana göre fonksiyonel, teknik ve güvenlik gereksinimleri testlerine tabi tutulur, test verileri özenle seçilerek korunur ve kontrol edilir.

i) Gerekli hallerde değiştirilmiş veya yeni geliştirilmiş sistem, gerçek ortamda kullanıma alınmadan önce, belirli bir olgunluk seviyesine ulaşana kadar eski sistemle beraber çalıştırılmasına devam edilir; bu şekilde paralel işletimin mümkün olmadığı durumlarda ise, değiştirilmiş veya yeni geliştirilmiş sistem belirli bir olgunluk seviyesine ulaşana kadar eski sistem veri kayıpsız olarak devreye alınabilir halde tutulur.

j) Bilgi sistemlerinin kullanımı ile ilgili gerekli eğitim materyalleri oluşturulur.

k) Geliştirme, test ve gerçek ortamdaki işlemler ile bu işlemlerin gerçekleştiği ortamlar, yetkisiz erişim ve değişim riskine karşı birbirinden ayrılır.

5.22 UYGULAMA GÜVENLİĞİ

Şirket, uygulamaların güvenli çalışmasını temin etmek amacıyla kontroller geliştirir. Bu kontroller girdi ve çıktı denetimini, hataların ele alınmasını, güncellemeleri, erişim denetimini, mobil uygulama ve API işletimine özgü konuları içerir ve asgari olarak kritik uygulamalarda ele alınır. Uygulama güvenliğine ilişkin esaslar **Uygulama Geliştirme Prosedürü**'nde açıklanmıştır.

Kimlik doğrulama verileri, kişisel ve finansal veriler ile benzeri hassas verilerin çerezlerde saklanması engellenir. Veri güvenliğini sağlamak amacıyla çerezler asgari sürelerde tutulur, kalıcı çerezlerin tutulma süresi güvenlik gereksinimlerine uygun olarak sınırlandırılır. Oturum çerezleri, oturum kapanışında otomatik olarak silinir. Çerezler her oturumda kullanıcıya özel olacak şekilde üretilir. Çerez değerlerinin her kullanıcı için benzersiz olması ve oturum açma sırasında yeniden üretilmesi sağlanır. Kullanılan çerezlerin, kullanıcının terminal cihazlarına yerleştirilmesi aracılığıyla otomatik yolla elde edilen kişisel verilerin hangi amaçlarla işlendiği ve hangi tür çerezler kullanıldığı ile kullanıcının bu çerezleri nasıl yönetebileceğine ilişkin bilgilere **Çerez Politikası**'nda yer verilmiştir.

Uygulamalarda geçici veya misafir kullanıcı erişimleri belirli süreler için sağlanır ve bu erişimler süre dolduğunda devre dışı bırakılır.

API erişimlerinde, kimlik doğrulama ve yetkilendirme için güvenli protokoller kullanılır. Erişim talepleri belirteç (token) bazlı doğrulanır ve kullanıcı kimlik bilgileri korunur. Zorunlu olmadıkça hassas verilerin API aracılığıyla iletilmesi engellenir.

API erişimlerinde aşırı yüklenme ve kötüye kullanım girişimlerine karşı trafik yönetimi yapılır. Bu kapsamda talep sınırlandırma ve yavaşlatma mekanizmaları kullanılır.

Uygulamaların oturum zaman aşımı süresi, uygulamanın kritikliğine göre belirlenir. Bu sürenin aşımında oturum otomatik olarak sonlandırılır ve kullanıcı yeniden giriş yapmaya zorlanır.

Uygulamanın kaynak kodlarının kötü amaçlı kullanım ve müdahalelere karşı korunaklı olması sağlanır.

Uygulamalarda, kullanıcı tarafından gönderilen tüm girdilerde kötü amaçlı içeriklerin tespit edilmesi ve engellenmesine yönelik kontroller tesis edilir ve bu amaçla koruma çözümleri kullanılır.

Uygulamalara yüklenen dosyaların güvenliğini sağlamak amacıyla dosya türü, boyutu ve içeriği kontrol edilir. Olası tehditlere karşı dosyalar, güncel zararlı yazılım imzalarına ve tehdit veri tabanlarına göre taranır, tespit edilen şüpheli dosyalar otomatik olarak karantinaya alınır veya yüklenmesi engellenir. Yüklenen dosyaların yalnızca yetkili kişilerce erişilebilmesi ve güvenliği sağlanır. Erişimlerin denetim izi tutulur.

5.23 BİLGİ SİSTEMLERİ GÜVENLİĞİ

Şirket faaliyetlerini destekleyen bilgi sistemlerinin sürekliliğini sağlamak üzere **İş Sürekliliği ve Acil Durum Eylem Planı**'nın bir parçası olan **Bilgi Sistemleri Süreklilik Planı** uygulanır.

Plan kapsamında ikincil sistem tesis edilir ya da bu hizmeti destek hizmeti kuruluşlarından tedarik etme hususunda güvence sağlayan anlaşmalar yapılır. İkincil sistemde, Şirket'in veri ve sistem yedekleri kullanıma hazır bulundurulur. Hizmetlerin tekrar kullanıma açılmasını sağlayacak alternatif kurtarma süreçleri planlanır ve gerekli önlemler alınır.

Performans Yönetimi ve Kapasite Planlaması Prosedürü çerçevesinde performans takibi ve kapasite planlaması yapılır, sistem kaynaklarının kullanımı izlenir. Bilgi sistemleri altyapısından kaynaklanabilecek kesintilere, işlem performansını düşürecek veya iş sürekliliğini aksatacak durumlara karşı gerekli önlemler alınır.

Birincil sistemlerin tamamen devre dışı kaldığı felaket senaryolarında dahi Şirket'in geç 24 (yirmi dört) saat içerisinde faaliyetlerini yeniden sürdürebiliyor olması esastır. Planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa gerçek bir felaket senaryosunu sağlamaya ve ikincil merkez üzerinden faaliyetleri sürdürmeye yönelik testler yapılır. Testlere varsa dış hizmet sağlayıcılar da dâhil edilir, test sonuçları Üst Yönetime raporlanır. Plan, test sonuçlarına göre ve iş süreçlerini veya bilgi sistemlerini etkileyecek değişikliklerden sonra gözden geçirilerek güncellenir.

Bilgi sistemleri, İş sürekliliği planındaki önceliklere uygun olarak yedeklenir ve yedekten geri dönülmesi için gerekli süreçler bilgi sistemleri sürekliliği planına ve testine dâhil edilir. Verilerin yedeklenmesine ilişkin esaslara **Yedekleme Prosedürü**'nde yer verilmiştir.

Şirket, bilgi güvenliği politikasının, bilgi sistemleri süreklilik planının, ağ topolojisinin, bilgi sistemleri varlık envanteri ile iş sürekliliği ve güvenliği açısından önem arz eden diğer dokümanların güncel sürümlerini ve bilgi sistemleri yönetimine ilişkin parolalarını güvenli ortamlarda saklar.

5.24 DEĞİŞİKLİK YÖNETİMİ

Şirket, bilgi sistemlerini oluşturan her türlü yazılım, donanım ve altyapı bileşenlerine, dokümantasyona ve bilgiye yapılan değişiklikleri yönetebilmek amacıyla **Değişiklik Yönetimi Prosedürü** çerçevesinde kontroller geliştirir. Bu kontroller en az aşağıdaki hususları içerir:

a) Yapılacak her türlü değişiklik için; değişikliğin sebebini, kapsamını, etkisini, içerdiği riskleri, beklenen faydasını, veri bütünlüğüne etkisini, değişikliği yapacak kişileri, maliyetini, gerekli test ve eğitim faaliyetlerini tanımlayan kayıtların oluşturulması ve onaylanması.

b) Değişikliğin talepten, test edilmesi, üretim ortamına aktarım ve kapanışına kadar yönetilmesi.

c) Planlanan değişikliklerin devreye alınma tarihleri, test ve eğitim faaliyetlerinin tüm taraflara önceden duyurulması.

d) Değişikliğin uygulanmasında ortaya çıkan hatalar ve öngörülemeyen durumlarda uygulamaya alınacak geri dönüş prosedürleri ve bunlarla ilgili sorumlulukların önceden belirlenmesi.

e) Gerçekleştirilen değişikliklerin sonuçları gözden geçirilir.

f) Gerçekleştirilen, iptal edilen veya reddedilen tüm değişikliklerin gerekçeleriyle birlikte kayda alınması.

5.25 BİLGİ GÜVENLİĞİ EĞİTİMLERİ

Şirket genelinde bilgi güvenliği farkındalık seviyesini artırmak için kapsamlı bir bilgi güvenliği farkındalığı eğitim programı oluşturulur. Eğitim programı, bilgi güvenliği politikaları ve standartları ile birlikte, bilgi güvenliği ve verilerin korunması konusundaki bireysel sorumlulukların neler olabileceği ve bilgi varlıklarını korumak için alınması gereken önlemler hakkında bilgi içerir. Bu eğitimler yoluyla Şirket'in bilgi teknolojileri kaynaklarına ve sistemlerine erişimi olan herkesin bu kaynakların kullanımı ile ilgili mevzuat ve ilgili diğer düzenlemeler hakkında bilgi sahibi olması sağlanır.

Bilgi güvenliği farkındalığı eğitim programı Bilgi Güvenliği Komitesi tarafından onaylanır ve programın içeriği yılda en az bir defa yeni teknolojiler ve ortaya çıkan yeni riskler dikkate alınarak gözden geçirilir ve güncellenir. Şirket'in bilgi teknolojileri kaynaklarına ve sistemlerine erişimi olan yeni ve mevcut personelin ve ilgili olduğu alanlar doğrultusunda bilgi teknolojileri kaynaklarına ve sistemlerine erişimi olan dış hizmet sağlayıcıların bu eğitimlerden geçmesi veya eğitimi aldıklarını belgelendirmeleri ve eğitim programı güncellendikçe ilgili kişilerin güncellenen kısımlarla ilgili yılda en az bir kere olmak üzere tekrar eğitim alması sağlanır.

Şirket, bilgi güvenliği farkındalığını artırmak üzere eğitim programının haricinde Şirket içi bilgilendirme materyalleri hazırlar, Şirket iç portalında bilgi güvenliği ile ilgili bir bölüm oluşturur, çalışanlara periyodik olarak bilgi güvenliğiyle ilgili hatırlatma mesajları gönderir, çalışanlara yönelik düzenli olarak bilgi güvenliği farkındalığını ölçecek anketler yapar.

Şirket farkındalık artırıcı çalışmaların etkinliğini doğrulamak ve geliştirilmesi gereken eksiklikleri tespit etmek amacıyla gerekli çalışmaları yapar. Güncel saldırı yöntemlerini dikkate alarak gerekli sosyal mühendislik senaryoları üzerinden çalışanlara yönelik periyodik testler gerçekleştirir ve bu testlerden geçemeyen çalışanlara yönelik ilave hedefli eğitimler verilmesini sağlar.

Şirket çalışanları, bilgi güvenliği ile ilgili sorumlulukları hakkında politikalar, prosedürler ve görev tanımları ile bilgilendirilirler.

Çalışanlara, iş sözleşmesinin imzalanması aşamasında, bilgi teknolojileri varlıklarına olan erişimleri ve bu varlıkları kullanımlarına ilişkin **Bilgi Güvenliği Taahhütnamesi** ile gizli bilgilerin güvenliğinin sağlanmasına yönelik **Gizlilik Taahhütnamesi** imzalatılır. Bu taahhütnamelerde çalışanların işten ayrılmaları durumunda dahi varlıkların ve bilginin korunmasına dair yükümlülüklerinin devam ettiğine ilişkin hükümler yer alır.

İş ilişkisi kurulan üçüncü taraflar ya da geçici olarak görevlendirilen çalışanların bilgi teknolojileri varlıklarına erişimlerinin öncesinde gizlilik anlaşmaları imzalanır.

5.26 DENETİM VE KONTROL

a) Bilgi Sistemleri Bağımsız Denetim Faaliyetleri

Kurul düzenlemeleri çerçevesinde, Kurul tarafından sermaye piyasasında bilgi sistemleri bağımsız denetimi yapmakla yetkilendirilmiş bağımsız denetim kuruluşları tarafından 2 yılda bir kez bilgi sistemleri bağımsız denetimi yaptırılır.

Bilgi sistemlerine ilişkin iç kontroller hakkında denetim dönemi itibariyle güvence veren ve Yönetim Kurulu tarafından onaylanmış olan yönetim beyanı Kurul'un Bilgi Sistemleri Bağımsız Denetim Tebliğinin 1 numaralı ekinde yer verilen hususları içerecek şekilde hazırlanır ve bilgi sistemleri denetçisine sunulur.

Bilgi sistemleri bağımsız denetim raporu, sorumlu bilgi sistemleri baş denetçisi tarafından imzalandığında kesinleşir. Bilgi sistemleri bağımsız denetim raporu kesinleşme tarihini izleyen ilk işgünü mesai bitimine kadar Şirket'e teslim edilir. Şirket Yönetim Kurulu Başkanlığınca teslim alınan bilgi sistemleri raporu en geç 5 işgünü içerisinde raporun kabulüne yönelik Yönetim Kurulu kararıyla birlikte Kurul'a gönderilir.

Bilgi sistemleri bağımsız denetim raporu, ilgili denetim döneminin bitimini izleyen 30 gün içinde tamamlanarak Kurul'a gönderilir. Bilgi sistemleri raporlarının son bildirim gününün resmî tatil gününe denk gelmesi halinde, resmî tatil gününü takip eden ilk iş günü, son bildirim tarihidir.

b) Bilgi Sistemleri İç Kontrol Faaliyetleri

Şirket ve Şirket'in dış hizmet sağlayıcıları nezdindeki bilgi sistemleri yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen bilgi sistemleri kontrollerinin ilgili mevzuata ve Şirket politika, prosedür ve standartlarına uyumlu olduğunu kontrol etmek ve Şirket Yönetim Kurulu'nun bilgi sistemlerine ilişkin iç kontrollerin bilgi sistemleri bağımsız denetim dönemi açısından etkinlik, yeterlilik ve uyumluluğuna ilişkin değerlendirmede bulunarak, mevcut durum ve yürütülen çalışmalara ilişkin güvence sunmasını temin etmek amacıyla, Şirket bünyesinde bilgi sistemleri iç kontrol faaliyetleri yürütülür.

Bilgi Sistemleri İç Kontrol Prosedürü çerçevesinde hazırlanan **Bilgi Sistemleri İç Kontrol Programı**, kapsamında, yapılan periyodik kontroller kayıt altına alınır ve yapılan kontrollere ilişkin çalışma kanıtları en az üç yıl Şirket nezdinde saklanır.

İç kontrol fonksiyonu ilave olarak aşağıdaki faaliyetleri de yerine getirir:

a) Kontroller sonucunda belirlenen eksikliklerin giderilmesi ve aksiyon alınması amacıyla ilgili birimlere ve Üst Yönetime bildirimde bulunulması,
b) Kontroller sonucunda gerekli olduğu anlaşılan süreçsel veya sistemsel iyileştirme önerilerinin ilgili birimlere ve Üst Yönetime bildirilmesi,
c) Talep halinde Şirket'in ürünlerinde ve süreçlerinde planlanan değişiklikler, yenilikler veya Şirket içi politika, prosedür ve süreç dokümanları hakkında görüş oluşturulması,
d) Görev alanına giren kritik süreçlerle ilgili proje ve çalışma gruplarına, kurul ve komitelere katılım sağlanması ve ilgili toplantılarda riski en aza indirmeye yönelik öneriler getirilmesi,
e) Bilgi teknolojileri yönetimi ve dış hizmet alımından kaynaklı risklerin takibinin sağlanmasına yönelik Üst Yönetime ve İç Denetim Birim Yöneticisine periyodik olarak raporlama yapılması,
f) Bir sonraki yıl yapılacak planlı incelemeleri gösterecek şekilde her yıl bilgi sistemleri iç kontrol inceleme planları oluşturulması ve bunların Şirket Yönetim Kurulu onayından geçirilmesi.

c) Bilgi Sistemleri İç Denetim Faaliyetleri

Şirket ve Şirket'in dış hizmet sağlayıcıları nezdindeki bilgi sistemleri yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen bilgi sistemleri kontrollerinin mevzuata ve Şirket içi politika, prosedür ve standartlara uyumlu olduğu ve bilgi sistemlerine ilişkin iç kontrol ve risk yönetimi faaliyetlerinin etkinliği ve yeterliliği hususunda Yönetim Kuruluna güvence sağlamak üzere bilgi sistemleri iç denetim faaliyetleri yürütülür.

İç denetimi gerçekleştirecek kişilerin Sermaye Piyasasında Faaliyette Bulunanlar İçin Lisanslama ve Sicil Tutmaya İlişkin Esaslar Hakkında Tebliğ (VII-128.7)'in 5 inci maddesinde belirtilen Bilgi Sistemleri Bağımsız Denetim Lisansına sahip olmaları zorunludur.

Yıllık olarak denetlenebilir bilgi sistemleri alanlarından oluşan bir bilgi sistemleri denetim planı oluşturularak Şirket Yönetim Kurulunun onayına sunulur. Şirket'in bilgi sistemleri asgari yılda en az bir kez olmak kaydıyla iç denetimlerinin sıklığı ve denetim döngüleri; bilgi sistemleri servislerinin, süreçlerinin ve varlıklarının kritikliği ve riski ile orantılı olarak iki yılı aşmayacak şekilde belirlenir.

Yapılan denetimlere ilişkin çalışma kanıtları en az üç yıl Şirket nezdinde saklanır.

d) Bulguların ve Aksiyonların Takibi

Şirket Yönetim Kurulu, bilgi sistemleri iç kontrol, iç denetim ve bağımsız denetim çalışmaları sonucu tespit edilen bulguların ele alınması konusuna yeterli zaman ayırır, bu çalışmalar sonucu tespit edilen kritik konuları bizzat gözden geçirir ve gerekli önlemlerin alınması konusunda Üst Yönetime rehberlik eder.

Şirket, iç kontrol ve denetim çalışmaları sonucu tespit edilen bulguların aksiyon planına bağlanarak takip edilmesini sağlar. Bulguların kapatılmasına yönelik olarak aksiyon planında hedef tamamlanma tarihi atanamayan, aşılan, aşma süresi bir seneden fazla uzatılan veya iptal edilen bulgular İç Denetim Birimi tarafından Yönetim Kuruluna düzenli olarak raporlanır ve bu bulgular Yönetim Kurulunda kritik konular olarak ele alınır.