GMS GLOBAL KRİPTO VARLIK

ALIM SATIM PLATFORMU A.Ş.

KURUMSAL BİLGİ GÜVENLİŞİ POLİTİKASI

1. AMAÇ VE KAPSAM

GMS GLOBAL KRİPTO VARLIK ALIM SATIM PLATFORMU A.Ş.("Şirket"), müşterilerinin sürekli güvenini hedeflemektedir. Bu güven aşağıdaki durumlarda hızla kaybedilebilir:

- Bilginin Şirketimiz dışına aktarılması veya çalınması
- Şirket bilgisinin değerini kaybedecek şekilde değiştirilmesi
- Bilginin yeniden elde edilemeyecek şekilde kaybedilmesi

Müşterilerimizin Şirket'e olan güveni, rekabet üstünlüğü yaratır. Söz konusu güven, bu bilgi güvenliği çalışmasının da dahil olduğu çabalar ile pekiştirilmeli ve geliştirilmelidir.

Bu politika dokümanı, asgari olarak aşağıdaki üç temel amacı kapsamaktadır:

Gizlilik – Bilginin, yetkisiz olarak ifşa edilmesinin engellenmesi. Bilgi, sadece ilgili kişilere ifşa edilir.

Bütünlük – Bilginin doğru ve eksiksiz olmasının sağlanması. Kayıtlar, yetkisiz kişiler tarafından veya yanlışlıkla oluşturulamaz, değiştirilemez veya imha edilemez.

Erişilebilirlik – Bilgi, yetkili kişiler tarafından kesintiye uğramadan her zaman kullanılabilir. Korunması gereken bilgiler bilgisayarlarda saklanabilir; ağ üzerinden iletilebilir; merkezi ya da dağıtık veritabanlarında depolanabilir; kağıt üzerine yazılabilir veya kağıt üzerinde basılı olabilir; faks ile gönderilebilir; teleks veya SWIFT yoluyla iletilebilir; kaset, disk veya diğer manyetik ortamlarda saklanabilir; görüşmelerde konuşulabilir (telefon dâhil); film ve mikrofişlerde saklanabilir; terminal ve iş istasyonlarında görüntülenebilir; tepegöz tarafından sunulabilir ve bilgi ve fikirleri nakletmek için kullanılan diğer yöntemler ile iletilebilir.

Bu politika, Şirketimiz bilgilerini yukarıda listelenen hususlara yönelik tehditlerden korumak, bilgi güvenliğini etkin olarak yönetmek, yürürlüğe girmesi beklenen düzenlemelere şimdiden uyum sağlamak düşüncesiyle örneklem olarak yürürlükte bulunan bankacılık ve finans kurumlarına ilişkin düzenlemeleri örnek almak ve uluslararası bilgi güvenliği standartlarına paralel çalışma prensipleri oluşturmak amacı ile geliştirilmiştir.

Bilgi Güvenliği Politikası, güvenlik önlemlerinin ana hatlarını ve Şirketimizin bilgi güvenliğine genel bakışını vurgulamaktadır.

2. GÜVENLİK POLİTİKASI

2.1 Giriş

Bu doküman, Şirket tarafından muhafaza edilen sınıflandırılmış veya sınıflandırılmamış tüm bilgilerin gizlilik, bütünlük ve kullanılabilirlik özelliklerinin korunmasına yönelik, Şirketimizin kurumsal bilgi güvenliği ve yönetimi politikasını ortaya koymaktadır. Bu politika, Şirketimizin tüm iş kollarının bilgi varlıklarını uygun şekilde korumalarını gerektirmektedir. Bu politika kapsamında ayrıca yine politika içerisinde detaylandırılan gerekliliklerin karşılanabilmesine yönelik sorumluluklar da açıklanmıştır. Bu politika Şirket, personeli ve tüm bilgi varlıklarının yeterli bir güvenlik düzeyine sahip olması için uygun bir zemin sağlar.

Kurumsal Bilgi Güvenliği Politikası, Yönetim Kurulu tarafından onaylanır.

2.2 Arka Plan

Şirket, bilgileri muhafaza etmek ve işlemek için ağırlıklı olarak teknolojik çözümlere bağımlıdır. Bu amaçla kullanılan sistemler gün geçtikçe daha karmaşık ve birbirine bağımlı hale gelmekte ve yeni teknolojinin ortaya çıkması nedeniyle, daha geniş bir yelpazedeki güvenlik risklerine maruz kalmaktadırlar. Bilgi sistemleri üzerine yapılan yatırımların ve bu sistemlere olan bağımlılığın korunabilmesi için güvenlik önlemleri hayata geçirilmelidir. Bu önlemler fiziksel, teknik ve personel güvenliği hususlarını içermektedir.

2.3 Amaç

Bilgi güvenliği politikasının amaçları aşağıda belirtilmiştir:

- Hizmetlerimizin gizlilik, bütünlük ve erişilebilirliğine yönelik tehditlere karşı Şirketimizin yeterince korunduğundan emin olmak. Güvenlik ihlalleri aşağıdaki sonuçları doğurabilir:
  - İtibar kaybı;
  - İş kaybı;
  - Varlık kaybı (veri, ekipman ve para dâhil olmak üzere);
  - Şirket aleyhinde yasal işlemlerin getireceği kayıp;
  - Kamu güveni, kredibilitesi veya saygısının kaybı;
- Bilgi güvenliği farkındalık düzeylerini artırmak ve bireysel sorumlulukların daha iyi anlaşılmasını sağlamak için tüm ortakları, yönetimi, personeli ve üçüncü partileri teşvik etmek;
- Genel kabul görmüş bilgi güvenliği ilkelerine ve beklenen yasal düzenlemelere uyum göstermek ve söz konusu uyumun devamlılığını sağlamak.

2.4 Kapsam

Bu politika, tüm seviyelerdeki Şirketimiz personeli (yarı-zamanlı ve tam-zamanlı personel, tedarikçiler ve herhangi bir sure zarfında Şirketimiz için çalışan üçüncü taraf personeli dâhil) için geçerlidir.

Bu politika kapsamındaki tehditler aşağıdakileri hedef alabilir:

- Müşteri adına veya dâhili amaçlarla Şirketimiz tarafından muhafaza edilen veya işlenen bilgi (matbu veya elektronik ortamda);
- Şirketimiz bilgilerinin işlendiği, Bilgi ağı, sistem ve uygulamaların da dahil olduğu, tüm bilgi işlem platformları;
- Şirketimiz personeli;
- Şirket binası ve tesisleri.

2.5 Politika Bildirimi

Şirketimizin güvenli bir şekilde hedeflerine ulaşabilmesi için, organizasyonumuz, politika ve prosedürlerimiz ve teknik faaliyetlerimiz, bilgi varlıklarının her koşulda kabul edilebilir gizlilik, bütünlük ve kullanılabilirlik düzeylerine sahip olmasını garanti altına alacak koruyucu önlemler ihtiva etmelidir.

Söz konusu koruyucu önlemler aşağıdaki hususları garanti etmeyi hedeflemektedir:

- Risk Yönetimi Birimi, Şirketimiz bilgi güvenliği ve iş sürekliliği süreçlerini tüm yönleriyle yönetmekten sorumludur;
- Bilgi Güvenliği Komitesi, Şirketimiz Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) uygulanmasına yardımcı olmak ve kolaylaştırmaktan sorumludur;
- Varlık ve operasyonların kayıp, hasar veya bozulmadan korunması amacıyla uygun ve etkili önlemler alınır;
- Önemli ve hassas bilgiler tanımlanır, sınıflandırılır ve söz konusu bilgiler kayıp, yetkisiz ifşa veya değiştirilmeye karşı korunur;
- Güvenlik zayıflıkları tespit edilir, değerlendirilir, kayıt altına alınır ve yönetilir; söz konusu zayıflıklardan kaynaklanan riskleri en aza indirmeye yönelik uygun tedbirler alınır;
- Şirket için iş sürekliliği planları hazırlanır, incelenir ve periyodik olarak test edilir;
- Gerçekleşen veya teşebbüste bulunulan güvenlik ihlalleri kayıt altına alınır, değerlendirilir ve yeniden vuku bulmalarını önlemek amacıyla ilgili güvenlik önlemleri iyileştirilir;
- Üzerlerinde mutabık kalınan, belirlenmiş müşteri güvenlik gereksinimleri karşılanır;
- Bilgi ve bilgi varlıklarına erişim hakkı, sadece görevleri gereği söz konusu bilgilere ihtiyaç duyan ve uygun yetki ve güvenlik onaylarına sahip kullanıcılar ile sınırlıdır;
- Tüm Şirketimiz personeli Kurumsal Bilgi Güvenliği Politikasının gerektirdiği ölçüde - bu politikaya yönelik uygulamaların bilincinde olup, yasal yükümlülükleri de dâhil olmak üzere bu politika kapsamındaki tüm sorumluluklarını bilmekte ve kabul etmektedirler;
- Bilgi güvenliğini sağlamaya yönelik tüm çalışmalar, bilgi güvenliğine ilişkin politikalar, standartlar ve prosedürlerin geçerli ve etkin olduklarını garanti altına almak amacıyla düzenli olarak gözden geçirilir.

Ayrıca, Risk Yönetimi Birimi Şirketimizin bilgi varlıklarını sürekli olarak izleyecek, bilgi güvenliğine yönelik politika ve prosedürleri oluşturacak ve güncelleyecek ve söz konusu düzenlemelerin tutarlı, zamanında ve maliyet-etkin bir şekilde hayata geçirildiklerinden emin olacaktır.

3. BİLGİ GÜVENLİŞİ ORGANİZASYONU

3.1 Organizasyon şeması

Bilgi güvenliği organizasyonu aşağıda gösterildiği şekilde yapılandırılmıştır. Bilgi güvenliğini planlama, yönetme ve operasyonel idaresi Bilgi Sistemleri Birimi'nin görevidir.

3.2 Bilgi Güvenliği Sorumluluklarının Dağılımı

Kurumsal Bilgi Güvenliği Politikası'nın başarılı bir şekilde uygulanması, tüm ancak çalışanlarımızın tam işbirliği ve desteği ile mümkün olabilir. Dolayısı ile tüm çalışanlarımızın belirlenen güvenlik gereksinimlerinin bilincinde olması ve bu gereksinimlere uygun davranmaları çok önemlidir. Bu doğrultuda, tüm çalışanlarımızın ilgili güvenlik prosedürlerine yönelik uygun eğitimleri almasını sağlamak ve yine bu prosedürlere uygun çalışmaları için gerekli ortamı oluşturmaktan Şirketimiz yönetimi sorumludur.

Operasyon ve Bilgi Teknolojileri Genel Müdürlüğü Yardımcılığı

Operasyon ve Bilgi Teknolojileri Genel Müdür Yardımcılığı, kapsamı ve hedefleri iş stratejisini destekleyecek şekilde yapılandırılmış, Şirket Bilgi Güvenliği Stratejisinin belirlenmesinden sorumludur. Operasyon ve Bilgi Teknolojileri Genel Müdür Yardımcılığı, aynı zamanda, bilgi güvenliği politikaları ve prosedürlerinin oluşturulması, uygulanması ve sürdürülmesinden, Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) geliştirilmesi, uygulanması ve sürdürülmesinden, çalışanlarımıza güvenlik ile ilişkili gereksinim ve sorumluluklarının iletilmesinden ve sistem ve erişim noktalarının izlenmesinden sorumludur. Ayrıca şirketimizin BT sistemlerinin güvenliklerinin devamlılığını sağlamaktan, bu sistemlerin düzenli olarak güvenlik açısından gözden geçirilmelerinden ve gerçekleşen veya potansiyel tüm bilgi güvenliği ihlallerinin, bilgi güvenliği koordinatörleri aracılığıyla Risk Yönetimi Birimi'ne bildirilmesinden sorumludur.

a. Bilgi Güvenliği tüzüğü ve aksiyon planı ile birlikte İş Stratejisi ile uyumlu olarak Bilgi Güvenliği Stratejisinin oluşturulması ve sürdürülmesi;
b. BT ve önemli iş birimleri ile birlikte İş Sürekliliği Planının hazırlanması, test edilmesi ve sürdürülmesi;
c. Şirket bünyesinde bilgi güvenliği standartları, politikaları ve prosedürlerin uygulanması ve etkinliğinin değerlendirilmesi;
d. Yazılım ve donanım satın alma ve kurulum süreçlerinde güvenlik değerlendirmelerinin yapılması;
e. Fiziksel güvenlik ve çevresel kontrollerin gözden geçirilmesi, değerlendirilmesi ve uygulanması;
f. Mantıksal erişim kontrollerinin, mümkün olan en az yetki ve görevler ayrılığı esaslarının sağlanması amacıyla, gözden geçirilmesi, değerlendirilmesi ve uygulanması;
g. Değişiklik yönetimi ve yedekleme süreçleri üzerindeki kontrollerin, gözden geçirilmesi değerlendirilmesi ve uygulanması;
h. Ödeme hizmetleri ve elektronik para kanalları ve dış hizmet alımı süreçleri üzerindeki kontrollerin gözden geçirilmesi ve değerlendirilmesi;
i. Bilgi güvenliği gözden geçirme çalışmalarının gerçekleştirilmesi;

Risk Yönetimi Birimi

a. Olağanüstü Durum Kurtarma planı ve Kurtarma Stratejisi'nin geliştirilmesinde yardım sağlanması;
b. Kullanıcılara bilgi güvenliği hakkında farkındalık eğitimi verilmesi ve rehberlik sağlanması;
c. Kritik faaliyetlerin ve bilgi güvenliği olaylarının izlenmesine (gerçekleşen olaylara ilişkin alınan aksiyonların takibi, kök neden analizi ve önceki olayların incelenmesi adımları da dahil olmak üzere) yönelik bir sürecin oluşturulması, hayata geçirilmesi ve sürdürülmesi;
d. Bilgi güvenliğine ilişkin yürürlükteki yasa ve düzenlemelere uyumun izlenmesi;
e. Gerektiğinde Genel Müdür ve Yönetim Kurulu'na Bilgi Güvenliği ve İş Sürekliliğine ilişkin faaliyetlerin raporlanması;
f. İş ve BT ile ilgili tarafların koordinasyonunun sağlanarak, BT varlık envanteri, veri sınıflandırma ve sahiplik tanımlarının oluşturulması;
g. Bilgi güvenliği gözden geçirme çalışmalarına yardım edilmesi

Bilgi Güvenliği Komitesi

Bilgi Güvenliği Komitesi, Şirket'in bilgi güvenliği ve gizliliği ile ilgili politika, prosedür ve girişimlerinin gözetilmesinden ve önceliklendirilmesinden sorumludur. Bilgi Güvenliği Komitesi, Kurumsal Bilgi Güvenliği Politikası hükümlerinin Şirketimiz tarafından muhafaza edilen tüm varlıklar için uygulanmasını sağlar ve bilgi güvenliği ile ilgili tüm çalışmalar için net bir yön ve yönetim desteği sağlar. Bilgi Güvenliği Komitesi, Risk Yönetimi Birimi, Operasyon Bilgi Teknolojileri Genel Müdür Yardımcısı, Bilgi Teknolojileri Müdürü'nden oluşur.

Komite Üyeleri

Komite üyeleri, Risk Yönetimi Birimi'ne destek olmaktan ve Şirketimiz ve müşteri bilgilerine ilişkin güvenlik gereksinimlerinin tespit edilmesinden, uygulanmasından, izlenmesinden ve gözden geçirilmesini sağlamaktan sorumludur.

Ayrıca, komite üyeleri "Bilgi Sahibi" rolüne sahip olup, bilgi varlıklarına, yetkili Bilgi Koruyucusu atama görevini de icra ederler.

Bilgi Koruyucuları

Bilgi Koruyucuları, yönetim tarafından kendilerine atanan bilgi varlıkları üzerindeki bilginin depolanmasından ve işlenmesinden sorumludur.

Şirket Personeli

Şirketimizin bilgi güvenliği politika ve prosedürlerinin farkında olmak ve tüm bu düzenlemelere uyumlu davranmak, tüm personelimizin sorumluluğudur.

3.3 Üçüncü Partiler

Üçüncü partilerin dahil olduğu iş süreçlerinden kaynaklanan Şirketimiz bilgi ve bilgi sistemlerine yönelik riskler, erişim hakkı verilmeden önce tespit edilmeli ve uygun kontroller hayata geçirilmelidir. Üçüncü partilerin Şirketimiz bilgilerine erişme, işleme, iletme veya yönetme ya da bilgi sistemlerine ürün veya hizmet eklemeye yönelik anlaşmalar, gerekli tüm güvenlik gereksinimlerini karşılamalıdır.

3.4 Bilgi Güvenliği Politikasının Gözden Geçirilmesi

Risk Yönetimi Birimi, bu dokümanı yılda bir defa veya iş ortamında ya da bilgi sistemlerinde önemli bir değişiklik sonrasında gözden geçirecektir. Gözden geçirme sonuçları onay alınması için Bilgi Güvenliği Komitesi ve sonrasında Yönetim Kurulu'na sunulacak ve daha sonra değişikliklerin hayata geçirilmesi amacıyla ilgili birimlere iletilecektir.

4. VARLIK YÖNETİMİ

4.1 Bilgi Varlıklarına Sorumluların Atanması

Amaç: Şirketimiz varlıklarının uygun şekilde korunması.

Politika: Şirket, varlıklarına değerleri ve önemleri ile orantılı koruma önlemleri sağlanacaktır. Bilgi sistemleri ile ilişkili önemli varlıklar için bir envanter hazırlanmalı ve bu envanterin güncelliği sağlanacaktır. Her varlığın mevcut lokasyonu ile bilgi güvenliği açısından kullanım kuralları açıkça

belirlenecek, sorumlu Bilgi Koruyucusu atanacak ve güvenlik sınıflandırması hesaplanacak ve dokümante edilecektir.

4.2 Bilginin Sınıflandırılması

Amaç: Bilgi varlıklarının uygun şekilde korunmasının sağlanması.

Politika: Şirket tarafından ve Şirket adına işlenen tüm bilgiler, kuruma özel (sahibi Şirket ise) veya mahrem (sahibi müşteri ise) olarak kabul edilecek ve uygun düzeydeki yönetimin resmi onayı olmadan Şirketimiz dışına ifşa edilmeyecektir.

Tüm bilgi ve verilere, gizlilik ve bütünlük derecelerine uygun koruma seviyeleri atanacaktır. Bu amaca yönelik olarak, bilgilerden sorumlu olan Bilgi Koruyucusu, bilgi güvenliği sınıflandırmalarının atanmasından sorumlu olacaktır. Söz konusu güvenlik sınıflandırması, tüm ilgili yasal ve düzenleyici gereklilikler doğrultusunda Şirketimizin bilgi sınıflandırma, saklama ve imha etme süreçlerini düzenleyen politika ve prosedürlerine uygun olarak gerçekleştirilecektir.

4.3 Bilginin Etiketlenmesi ve Muhafazası

Amaç: Personelimize bilgi varlıklarının hangi seviyede korunmaları gerektiği bilgisinin aktarılması.

Politika: Bilgilerin (fiziksel ve elektronik ortamlardaki) etiketlenmesi ve muhafazasına yönelik prosedürler, Şirketimiz tarafından kabul edilen bilgi sınıflandırma kriterlerine uygun olarak, oluşturulacaktır. . Her sınıflandırma derecesi için, ilgili bilginin kopyalanması, depolanması, iletimi ve imha edilmesi süreçlerini detaylandıran bilgi muhafazası prosedürleri oluşturulacaktır.

Sınıflandırılmış bilgi içeren sistemlerin çıktıları, bu doğrultuda uygun bir sınıflandırma etiketi taşıyacaktır.

Veriyi ve/veya bilgiyi kontrol eden kişi söz konusu bilginin güvenliğinden de sorumlu olacaktır; ancak aşağıdaki hususları düzenleyen prosedürler tüm Şirket genelinde tek ve ortak olacaktır:

- Veri sınıflandırma
- Veri saklama ve imha etme
- Güvenlik ihlalleri ve erişim yetkilerinin kayıt altına alınması

5. İNSAN KAYNAKLARININ GÜVENLİŞİ

5.1 İş Tanımı ve İnsan Kaynağı Güvenliği

Amaç: İnsan hatası, hırsızlık, dolandırıcılık ya da Şirketimiz tarafından sağlanan ekipman, tesis ve/veya olanakların kötü amaçlar doğrultusunda kullanılması risklerinin en aza indirgenmesi.

Politika: İnsan faktörü ile ilişkili riskler aşağıdaki önlemler yolu ile hafifletilecektir:

- Şirketimiz Etik kurallarına sıkı bağlılık;
- İşe alım sürecinde adayların özgeçmiş doğrulamasının yapılması;
- Çalışanlarımızın iş amaçlı bulundukları lokasyonlara ilişkin kesin bilgilerin takip edilmesi;

- Güvenlik olayları ve sistemsel hatalara müdahale edilmesi sürecini içeren prosedürlerin oluşturulması ve güncel tutulması;
- Güvenlik ihlalleri için resmi disiplin süreci.

Personelimiz de, bazı durumlarda, Şirketimizin bilgi güvenliğine yönelik bir tehdit oluşturabilir. İşe alma ve istifa / işten çıkarılma prosedürleri, Şirketimizin personel kaynaklı tehditler ile ilişkili güvenlik zaaflarını azaltmaya yönelik şekilde tasarlanacaktır.

Şirketimiz güvenlik kurallarına uygun davranılması iş sözleşmesinin bir gerekliliğidir.

Şirket'e hizmet sağlayan firmalar ile yapılan sözleşmeler kapsamında, firma personelinin, Şirketimizce uygulanan bilgi güvenliği tedbirlerinin (standart, politika ve prosedür gibi) de dahil olduğu, uygun güvenlik kurallarını takip edeceğini belirttiği bir madde bulunacaktır.

5.2 Eğitim ve Farkındalık

Amaç: Personelimizin bilgi güvenliği tehditlerinin bilincinde olduğundan ve günlük çalışmaları esnasında Kurumsal Bilgi Güvenliği Politikasını uygulayabilecek yeterlilikte olduklarından emin olunması.

Politika: Personelin bilgi güvenliği ile ilgili prosedürler konusunda yeterli seviyede eğitim almış olmasını sağlamak birim yöneticilerinin sorumluluğundadır.

Bilgi güvenliği farkındalığı ve bilgi güvenliğine ilişkin prosedürlerin eğitimi tüm yeni istihdam edilen personel için sağlanacak ve tüm personelimiz için periyodik güncelleme eğitimleri düzenlenecektir.

Bilgi güvenliğine ilişkin özel rolleri olan personel için, ihtiyaç halinde, gerekli eğitimler Risk Yönetimi Birimi tarafından verilecektir.

Tüm personel, Kurumsal Güvenlik Politikasını ve ilgili prosedürleri (yasal yükümlülükleri dâhil) okuduğunu, anladığını ve sorumlu olduğunu belirttiği bir onay bildirimi imzalayacaktır.

5.3 İstihdamın Sona Ermesi

Amaç: Personelin ve üçüncü parti çalışanlarının Şirket'ten uygun bir şekilde ayrıldığından veya görevlerinin değiştirildiğinden emin olunması.

Politika: İstihdamın sona ermesi veya görev değişikliği yapılması sürecindeki sorumluluklar açıkça tanımlanacak ve ilgili personele atanacaktır. Tüm personel ve üçüncü parti çalışanları, istihdam, anlaşma veya sözleşmenin sona ermesi durumunda kendilerine verilen Şirket varlıklarını iade edeceklerdir. Ayrıca, söz konusu kişilerin bilgi ve bilgi sistemlerine erişim hakları derhal iptal edilecektir.

5.4 Bilgi Güvenliği İhlallerine Yönelik Disiplin Cezaları

Amaç: Bilgi güvenliği ihlallerinde doğru disiplin yaptırımlarının uygulanması.

Politika: Bilgi sistemleri ve bilgi sistemlerine erişimi olan Şirketimiz çalışanları ve tedarikçiler tarafından gerçekleştirilen Kurumsal Bilgi Güvenliği Politikası ve ilişkili prosedürlerin ihlalleri (kasıtlı veya yanlışlıkla), gerekli disiplin işleminin başlatılması amacıyla, sorumlu Direktör ve Risk Yönetimi Birimi'ne bildirilecektir.

Harici kaynaklı olay ve tehditler için, olaya ilişkin kanıtların yasalar karşısında kabul görürlüğünü zedelemeyecek şekilde aksiyon alınacak ve gerek görüldüğü durumlarda yasal işlemler başlatılacaktır.

6. FİZİKSEL VE ÇEVRESEL GÜVENLİK

6.1 Güvenli Alanlar

Amaç: Şirketimiz binası ve bilgilerine yetkisiz fiziksel erişimlerin ve zararın önlenmesi.

Politika: Güvenli alanların sınırları net olarak tanımlanacak ve sınırlı erişim gerektiren alanlar uygun fiziksel ve çevresel kontroller yoluyla korunacaktır. Şirket tesisleri ve fiziksel varlıklarına yetkisiz erişimlerin ve suistimal edilmelerinin önlenebilmesi amacıyla etkili güvenlik önlemleri hayata geçirilmeli ve düzenli olarak incelemeye tabi tutulmalıdır. Söz konusu güvenlik önlemleri, en azından; ziyaretçi kontrolü, mal teslimi, Şirket varlıklarının tesislerin dışına çıkartılması ve güvenli alanlara erişim yetkisi verilmesi hususlarını kapsamalıdır.

6.2 Ekipman Güvenliği

Amaç: Şirketimiz varlıklarının çalınmasının, zarar görmesinin veya riske maruz kalmasının ve bu doğrultuda Şirketimiz faaliyetlerinin kesintiye uğramasının önlenmesi.

Politika: Şirketimiz çalışanları tarafından kullanılan tüm ekipmanlar ve bilgi varlıkları, uygun erişim kontrollerine tabi tutulacaktır. Ekipmanlar yetkisiz erişime ve çevresel tehditlere karşı korunacak ve düzenli olarak bakımları gerçekleştirilecektir. Tüm ekipmanların çalınması, tahrip edilmesi ve suiistimal edilmelerinin engellenmesine yönelik kontrolleri içeren düzenlemeler oluşturulacak ve söz konusu düzenlemelere uyum sağlandığı garanti altına alınacaktır. Şirketimiz kaynakları sadece Şirket çalışmaları ile kullanılacaktır.

6.3 Genel Kontroller

Amaç: Bilginin çalınmasının ve bilgi veya bilgi sistemlerinin riske maruz kalmalarının önlenmesi.

Politika: Yetkisiz erişim, bilgi kaybı ve bilginin zarar görmesi tehditlerinin, normal çalışma saatleri içerisinde ve sonrasında, en alt seviyeye indirilmesi amacıyla, , matbu dokümanlar ve taşınabilir veri depolama aygıtları için bir temiz masa politikası ve bilgi sistemleri için bir temiz ekran politikası oluşturulacaktır. Müşteri ile ilgili tüm hassas bilgiler ve Şirket içi çalışmalar veya dokümanlar, mesai saatleri sonrasında ve hafta sonları kapalı dolaplarda saklanacaklardır. Özellikle kıymetli evraklar ve tek kopya dokümanların saklanması için yanmaz dolap veya kasalar, kullanılacaktır. Şirket'e ait ekipman, bilgi, yazılım ya da donanımın, uygun bir yönetim seviyesinden resmi izin olmadan, yeri değiştirilemez.

7. İLETİŞİM VE OPERASYON YÖNETİMİ

7.1 Operasyonel Prosedürler ve Sorumluluklar

Amaç: Bilgi sistemlerinin doğru ve güvenli çalışmasının sağlanması.

Politika: Bilgi sistemlerinin yönetilmesi ve işletilmesi ile ilgili tüm sorumluluklar ve prosedürler oluşturulacak ve gerekli şekillerde güncellenecektir. Söz konusu düzenlemeler çalışma talimatnameleri ve olay müdahale prosedürlerinin yanı sıra bilgi sistemlerinin geliştirilmesi, test edilmesi ve gerçek ortama aktarılmaları süreçlerini de kapsayacaktır.

Bilgi sistemlerinin ihmalen veya kasıtlı olarak kötüye kullanılmalarını engellemek amacıyla, görevler ayrılığı ilkesi tam ve doğru bir şekilde hayata geçirilecektir.

7.2 Üçüncü Parti Hizmetlerinin Yönetimi

Amaç: Üçüncü parti hizmet anlaşmaları için, uygun güvenlik önlemlerinin hayata geçirilmesi ve söz konusu önlemlerin sürdürülmesi.

Politika: Tüm destek hizmet sözleşmeleri, yürürlükteki yasa ve düzenlemelere ilişkin gereklilikleri karşılayan hükümleri içerecektir. Üçüncü partiler tarafından sağlanan hizmetler, söz konusu hizmetlere ilişkin sözleşmelerde tanımlanmış olan uygun güvenlik kontrolleri, tanımları ve hizmet seviyelerinin hayata geçirildiğinden emin olunması amacı ile, düzenli olarak izlenecek, gözden geçirilecek ve denetlenecektir. Hizmetlerin sunulmasına ilişkin gerçekleştirilmek istenen büyük ya da küçük değişiklikler, etkilenecek sistem ve süreçlerin önemleri dikkate alınarak, ancak uygun yazılı iznin ardından hayata geçirilecektir.

7.3 Sistem Planlama ve Kabul

Amaç: Sistem hatalarının en aza indirilmesi.

Politika: Kullanılabilir kapasite ve kaynakların yeterliliğinin sağlanabilmesi amacıyla, , ileriye dönük planlama ve çalışmalar yapılacaktır. Gelecekte sistem kapasitelerinin yetersiz kalması riskini bertaraf etmek amacıyla geleceği yönelik kapasite ihtiyaç projeksiyonları gerçekleştirilecektir. Yeni sistemler kabul edilerek kullanılmaya başlanmadan önce, söz konusu sistemlerin operasyonel gereksinimleri belirlenecek, dokümante edilecek ve test edilecektir.

7.4 Kötü Niyetli ve Mobil Koda Karşı Koruma

Amaç: Yazılımların ve bilginin bütünlüğünün korunması

Politika: Kötü amaçlı ve hatalı yazılımları belirlemek, bu yazılımlara karşı korunmak, virüs ve diğer zararlı kodların yayılmasını engellemek ve bu zararlı kodların yayılması ile oluşabilecek hasarları önlemek amacıyla prosedürler oluşturulacaktır. Mobil kod kullanımına izin verilen durumlarda, söz konusu kodların önceden belirlenmiş bir güvenlik politikasına göre çalışacaklarından ve yetkisizi mobil kodların çalışmasını engelleyici kuralların hayata geçirilmiş olduğundan emin olunacaktır.

7.5 Yedekleme

Amaç: Bilgi ve bilgi sistemlerinin bütünlüğünün ve kesintisiz kullanılabilirliğinin sürdürülmesi.

Politika: Onaylanan yedekleme stratejisinin hayata geçirilmesi, bilgi ve yazılımların yedeklerinin alınması ve geri yükleme testlerinin yapılması (hataların kayıt izlerinin saklanması da dahil olmak üzere) ve yedeklemeye ilişkin ekipmanların sürekli olarak izlenmesine yönelik aktiviteleri detaylandıran prosedürler oluşturulacaktır.

Bilgi ve yazılımların yedekleri, düzenli aralıklarla alınacak ve söz konusu yedeklerin ikinci bir kopyaları ana veri işleme tesislerinden farklı bir coğrafi konumda bulunan alternatif bir lokasyonda, korumalı bir ortamda, muhafaza edilecektir. Tüm yedeklenen verilerin saklama süreleri, iş ve yasal gereksinimlere uygun olacak şekilde belirlenecektir.

7.6 Bilgi Ağı Güvenliği Yönetimi

Amaç: Bilgi ağları yoluyla iletilen bilginin ve bilgi ağlarını oluşturan altyapının korunması.

Politika: Bilgi ağları, tehditlere karşı korunabilmeleri ve aralarında iletişimi sağladıkları sistem ve uygulamalarda güvenliğin sağlanabilmesi amacıyla, uygun bir şekilde yönetilecek ve kontrol edilecektir. Hassas verilerin dahili veya harici bilgi ağları aracılığı ile iletildiği durumlarda, söz konusu verileri yetkisiz erişime karşı koruyacak prosedürler hayata geçirilecektir.

Şirketimiz sistemlerine dışarıdan gerçekleştirilen uzaktan erişimlere yönelik talepler, sıkı bir şekilde sınırlandırılacak ve hem Operasyon ve Bilgi Teknolojileri Genel Müdür Yardımcılığı hem de Risk Yönetimi Birimi tarafından izlenecektir. Benzer şekilde, Şirketimiz tarafından üçüncü partiler ile iletişim için uzaktan erişim metotları kullanıldığı durumlarda sadece izin verilen verilerin iletişiminin gerçekleştirildiğini garanti altına alacak kontroller hayata geçirilecektir. Ayrıca, Şirket ağlarına yapılan tüm kablosuz erişim bağlantıları, iş ihtiyaçları dikkate alınarak değerlendirilecek ve onaylanacak; söz konusu bağlantılar uygun güvenlik standartlarına göre oluşturulacaktır.

7.7 Ortam Yönetimi

Amaç: Bilgi varlıklarının yetkisiz ifşa, değiştirilme, silinme veya imha edilmesinin ve iş faaliyetlerinin kesintiye uğramasının önlenmesi.

Politika: Bilgi varlıklarını barındıran tüm ortamlar kontrol altında tutulacak ve fiziksel olarak korunacaktır. Dokümanlar, bilgisayarlar, girdi/çıktı verileri ve sistem dokümantasyonlarının hasar, hırsızlık ve yetkisiz erişimden korunması amacıyla, uygun çalışma talimatnameleri oluşturulacaktır. Tüm bilgisayarlar, elektronik ortamlar ve dijital cihazlar atılmadan önce barındırdıkları verilerden arındırılacaktır. Kullanılan arındırma yöntemleri, bilginin, yeniden elde edilmesini engelleyecek şekilde, tanınmayacak hale gelmesini garanti altına alacaktır. Hassas verilerin bulunduğu karbon kağıt, yazıcı şeridi, manyetik kasetler ve diskler gibi atık malzemeler mümkün olan en kısa sürede uygun arındırma yöntemleri kullanılarak imha edilmelidir.

7.8 Bilgi İletimi

Amaç: Şirketimiz içerisinde veya Şirketimiz ile diğer kuruluşlar arasında iletilen bilgi ve yazılımların güvenliğinin sağlanması.

Politika: Bilgi ve yazılımların, Şirketimiz içerisinde veya Şirketimiz ile diğer kuruluşlar arasında, elektronik ve manuel iletiminin korunmasına yönelik resmi bilgi iletim politika, prosedür ve kontrolleri oluşturulacak ve hayata geçirilecektir.

Aktarım halindeki ortamları (bilgi varlıklarını barındıran) veya iletilen elektronik ve fiziksel verileri yetkisiz kişilerin erişiminden, kötüye kullanılmalarından veya kasıtlı olarak bozulmalarından korumaya yönelik prosedürler oluşturulacaktır.

7.9 Elektronik Posta Güvenliği

Amaç: Elektronik posta ile ilgili iş ve güvenlik risklerini azaltılması ve Şirketimizin kurumsal itibarının korunması.

Politika: Şirket'in e-posta sistemi, kullanıcılara sadece iş yapmaları için gereken ihtiyaca karşılık sunulacaktır.

Gizli ve sınırlı olarak sınıflandırılan bilgi ve belgeler, kriptolu olmadıkça ve alıcı söz konusu bilgi ve belgeleri görmek için yetkili olmadıkça, İnternet üzerinden e-posta olarak gönderilmeyecektir.

Çalışanlarımız, küçük düşürücü, taciz olarak nitelendirilebilecek veya profesyonel olmayan e-postalar veya uygunsuz/yasaklanmış e-posta ekleri göndermeyeceklerdir.

Tüm iş e-postaları Şirket kaydı olarak kabul edilecektir. Internet üzerinden gönderilen tüm e-postalara, Bilgi Güvenliği ve Hukuk Departmanları tarafından onaylanan feragatname mesajı eklenecektir.

7.10 Elektronik Ticaret Hizmetler

Amaç: Elektronik ticaret hizmetlerinin güvenli kullanımlarının sağlanması.

Politika: Hesap hareketlerine ilişkin çevrimiçi işlemler, söz konusu işlemlerin sunumunda kullanılan Internet siteleri de dahil olmak üzere, hatalı iletimleri, bozulmuş yönlendirmeleri, , yetkisiz mesaj değiştirilmesini, yetkisiz ifşayı, yetkisiz mesaj çoğaltılmasını veya iletilmesini önleme amaçlı uygun güvenlik kontrolleri hayata geçirilecektir.

7.11 İnternet ve Mobil Uygulama Güvenliği

Amaç: İnternet kaynaklarına erişimin, söz konusu kaynakların kullanım ve güvenliklerinin yönetilmesi.

Politika: İnternete erişim talepleri, birim yöneticileri tarafından onaylanacak ve Risk Yönetimi Birimi'ne bildirilecektir. İnternet erişimi, kalıcı veya geçici, yalnızca söz konusu erişim hakkına ihtiyacı olan personele sağlanacaktır. İnternetten indirilen tüm dosyalar (veritabanları, yazılım kaynak kodu, elektronik tablolar, dosyalar vb), indirme metodundan bağımsız olarak (e-posta eki veya ftp) belirlenen virüs tanımlama yazılımı ile taranacaktır.

İnternet üzerinden alınan veya gönderilen tüm bilgiler, dijital imza veya benzeri teknolojiler vasıtası ile doğrulanacaktır.

Şirketimize ait gizli, sınırlı veya özel olarak sınıflandırılmış bilgiler, onaylanan yöntemlerle kriptolanmadıkları sürece, İnternet üzerinden iletilmeyeceklerdir.

7.12 İzleme

Amaç: Yetkisiz bilgi işlem faaliyetlerinin tespit edilmesi.

Politika: Yönetici ve sistem operatörleri de dahil olmak üzere, bilgi sistemleri üzerindeki kullanıcı aktivitelerinin iz kayıtları tutulacaktır. Ayrıca, çalışanlarımız ile üçüncü parti ve tedarikçi kullanıcıları tarafından gerçekleştirilen İnternet aktiviteleri, yürürlükteki yasa ve düzenlemelere uygun olarak, kayıt altına alınacaktır. Yüksek yetkili kullanıcıların işlemlerine ilişkin iz kayıtları, normal kullanıcı iz kayıtlarına nazaran, ek bilgiler ve detaylar içerecek şekilde tutulacak ve yine özel olarak izlenecektir.

Güvenlik olaylarına ilişkin kayıtlar, periyodik olarak gözden geçirilecek, analiz edilecek ve uygun aksiyonların alınması sağlanacaktır. İz kayıtları (aktivite, erişim ve güvenlik kayıtları), yürürlükteki yasa ve düzenlemelere uygun olarak, ihtiyaç halinde sonraki araştırmalarda kullanılmak üzere belirli bir süre boyunca saklanacaklardır. Söz konusu kayıtlar, yetkisiz erişim veya değiştirilmeye karşı korunacaklardır.

Tüm bilgi sistemlerinin saatleri, kayıt bilgilerinin tutarlılığını sağlamak amacıyla, senkronize edilecektir.

8. ERİŞİM KONTROLÜ

8.1 Erişim Kontrolüne İlişkin İş Gereksinimleri

Amaç: Bilgiye erişimin kontrollü olarak sağlanması.

Politika: Bilgi ve iş süreçlerine erişim hakları iş ve güvenlik gerekliliklerine dayalı olarak (bilgi dağıtım ve yetkilendirme politika ve prosedürleri dikkate alınarak) yönetilecektir.

Tüm uygulamalar için bir erişim yönetim sistemi oluşturulacak ve erişim talepleri doğrulama veya değerlendirme ve konsolidasyon amaçlı olarak sorumlu birimlere iletilecektir.

8.2 Kullanıcı Erişim Yönetimi

Amaç: Bilgi sistemlerine sadece yetkili kullanıcıların erişmesinin sağlanması.

Politika: Bilgi sistemleri ve hizmetlere erişim haklarının kontrol edilmesine yönelik prosedürler hayata geçirilecektir. Söz konusu prosedürler, yeni kullanıcının ilk defa oluşturulması aşamasından, bilgi sistemleri ve hizmetlere erişim ihtiyacının ortadan kalkması ile kaydının silinmesi aşamasına kadar olan, kullanıcı erişim yaşam döngüsünün tüm aşamalarını kapsayacaktır. Normal sistem kontrollerini geçersiz kılabilen ayrıcalıklı kullanıcıların erişim haklarının atanması sürecine özel önem verilecektir.

Bilgi sistemlerine yetkisiz erişimi engellemek ve "en az ayrıcalık" ile “görevler ayrılığı” ilkelerinin sürdürülmesini sağlamak amacıyla, yılda iki kere veya ihtiyaç olduğunda, kullanıcı hesaplarının incelenmesine yönelik resmi bir süreç oluşturulacak ve hayata geçirilecektir.

8.3 Kullanıcı Sorumlulukları

Amaç: Yetkisiz kullanıcı erişiminin ve bilgi ve bilgi sistemlerine yönelik hırsızlık veya diğer risklerin önlenmesi.

Politika: Etkili bir güvenliğin kurulması için yetkili kullanıcıların bu yönde işbirliği yapması zorunludur. Kullanıcılar, özellikle şifrelerin atanması ve kullanıcı ekipman güvenliği hususlarında, etkili erişim kontrollerinin sürdürülebilmesi için üzerlerine düşen sorumluluklarının farkında olacaklardır.

Kendilerine bir kullanıcı kodu ve şifre atanmış kullanıcılar, söz konusu kod ile gerçekleştirilecek tüm işlemlerden sorumlu tutulacakları hususunun farkında olacaklar ve bu doğrultuda şifrelerini güvenli bir şekilde muhafaza edeceklerdir.

8.4 Bilgi Ağı Erişim Kontrolü

Amaç: Ağ hizmetlerine yetkisiz erişimlerin engellenmesi.

Politika: Dahili ve harici ağ servislerine erişimler kontrollü olarak sağlanacaktır. Ağlar ve ağ hizmetlerine erişimi olan kullanıcıların ağ hizmetlerinin güvenliğini tehlikeye atmamalarını sağlamak amacıyla aşağıdaki hususlar garanti altına alınacaktır:

- Şirket ağı ile diğer kuruluşlara ait ağlar veya umumi ağlar arasında güvenli arayüzler;
- Lokal ve uzaktan erişen kullanıcılar ve ekipmanlar için uygun bir kimlik doğrulama mekanizması;
- Bilgi hizmetlerine kullanıcı erişimlerinin kontrolü.

8.5 İşletim Sistemi Erişim Kontrolü

Amaç: İşletim sistemlerine yetkisiz erişimin engellenmesi.

Politika: Bilgisayar kaynaklarına erişimin kontrol altına alınması amacıyla güvenli oturum açma yöntemleri kullanılacaktır.

Tüm çalışanlarımız veya Şirketimiz bilgi sistemlerine erişmek üzere yetkilendirilmiş üçüncü partiler, söz konusu erişimi kendilerine atanmış olan benzersiz bir kullanıcı kimliği ve karşılık gelen bir şifre (söz konusu şifre ilk oturum açıldıktan sonra otomatik olarak değiştirilmeye zorlanacaktır) ile gerçekleştireceklerdir. Sistem kaynaklarının korunması ve yetkisiz erişimlerin engellenmesi için uygulamalar belirli bir hareketsizlik süresinden sonra otomatik olarak oturumu kapayacak şekilde ayarlanacaktır.

8.6 Uygulama ve Bilgi Erişim Kontrolü

Amaç: Uygulama sistemlerinde tutulan bilgilere yetkisiz erişimin engellenmesi.

Politika: Hassas bilgi sistemlerine erişimin kısıtlanması amacıyla mantıksal ve fiziksel güvenlik kontrolleri uygulanacaktır. Mantıksal ve fiziksel erişimler, kullanıcıların iş fonksiyonlarına bağlı olarak sınırlandırılacaktır.

8.7 Sistem Erişimi ve Kullanımını İzleme

Amaç: Sistem erişimleri ve kullanımlarına ilişkin izinsiz faaliyetlerin tespit edilmesi.

Politika: Erişim kontrolü politikasına aykırılıkların tespit edilmesi amacıyla Sistemler izlenecek, olağan dışı olaylar, bir güvenlik olayı olma olasılığına karşın, kanıt teşkil edecek şekilde kayıt altına alınacaktır. Risk Yönetimi Birimi sistem erişimlerini ve kullanımlarını düzenli olarak izleyecektir.

8.8 Taşınabilir Bilgisayar ve Uzaktan Çalışma

Amaç: Taşınabilir bilgisayar ve uzaktan çalışma olanaklarının kullanılması esnasında bilgi güvenliğinin sağlanması.

Politika: Taşınabilir bilgi işlem ve iletişim olanaklarının kullanmasına bağlı olarak ortaya çıkan risklerin en az seviyeye indirilmesine yönelik güvenlik önlemleri alınacaktır. Uzaktan çalışmalar için, Şirket uygulanabilir durumlarda, uzaktan çalışma lokasyonunda gerekli güvenlik önlemlerini alacak ve gerekli düzenlemelerin yerinde olmasını sağlayacaktır. Taşınabilir bilgisayar kullanılması durumlarında, Şirket, taşınabilir bilgi işlem cihazları ve temel altyapıyı korumak için yeterli mantıksal ve fiziksel güvenlik kontrollerini sağlayacaktır.

9. BİLGİ SİSTEMLERİ SATIN ALMA, GELİŞTİRME VE BAKIM

9.1 Bilgi Sistemlerinin Güvenlik Gereksinimleri

Amaç: Güvenliğin, bilgi sistemlerinin ayrılmaz bir parçası olmasının sağlanması.

Politika: Bilgi sistemlerinin geliştirme çalışmasına başlanmadan önce güvenlik ihtiyaçları belirlenecek üzerlerinde mutabık kalınacaktır. Tüm güvenlik gereksinimleri, gerçek ortama aktarımdan geri dönüş uygulamaları da dahil olmak üzere, projenin ihtiyaç analizi aşamasında belirlenecek ve söz konusu gereklilikler iş ihtiyacının bir parçası olarak gerekçelendirilecek, onaylanacak ve dokümante edilecektir.

9.2 Uygulamaların Doğru İşlemesi

Amaç: Uygulamalar yoluyla bilgide meydana gelebilecek hata, kayıp, yetkisiz değişiklik ve kötüye kullanmaların önlenmesi

Politika: Tüm uygulamalar, kullanıcılar tarafından geliştirilen uygulamalar da dahil olmak üzere, için uygun kontroller ve denetim izleri / aktivite iz kayıtları tasarlanacaktır. Söz konusu kontroller, en azından, veri girişi, hesaplama kontrolleri, mesaj bütünlüğü ve çıkış verisinin doğrulanmasını içerecektir.

Hassas, değerli veya kritik bilgi varlıkları üzerinde etkiye sahip olan sistemler için ek kontroller gerekli olabilecektir. Bu tür kontroller güvenlik gereksinimleri ve risk değerlendirmelerine dayalı olarak geliştirilecektir.

9.3 Kriptolojik Kontroller

Amaç: Bilgilerin gizliliği, orijinalliği veya bütünlüğünün kriptolama yoluyla korunması.

Politika: Risk altında olduğu ve söz konusu riskin diğer kontroller ile yeterli seviyede indirgenemediğine kanaat getirilen bilgilerin korunması için kriptolama sistem ve teknikleri kullanılacaktır.

9.4 Sistem Dosyalarının Güvenliği

Amaç: Sistem dosyalarının güvenliğinin sağlanması.

Politika: Gerçek ortamdaki sistemler üzerine yazılım yüklenmesi, sadece yetkilendirilmiş BT personeli ile sınırlandırılacaktır. Verilere erişim, program kaynak kodları ve sistemlere erişim, uygun koruma sağlanması amacıyla kontrol altında tutulacak ve yönetilecektir.

9.5 Uygulama Geliştirme ve Destek Süreçlerinde Güvenlik

Amaç: Bilgi ve uygulamaların güvenliğinin sağlanması.

Politika: Gerçek ve test ortamları sıkı bir biçimde kontrol edilecektir. Uygulamalardan sorumlu yöneticiler, gerçek ve test ortamlarının güvenliğinden sorumlu olacaklardır. Önerilen tüm yazılım değişiklikleri, Şirket operasyonları veya güvenlik önlemleri üzerinde olumsuz etkileri bulunmadığının garanti altına alınması amacıyla, incelemeden geçirilecek ve test edilecektir.

9.6 Teknik Güvenlik Açıklıkları Yönetimi

Amaç: Bilinen teknik güvenlik açıklarının istismar edilmesinden kaynaklanan risklerin azaltılması.

Politika: Operasyon ve Bilgi Teknolojileri Genel Müdür Yardımcılığı, bilinen güvenlik açıkları sebebiyle karşı karşıya olunan tehditleri, söz konusu tehditler istismar edilmeden, en aza indirmek için gerekli önlemleri ve tedbirleri alacaktır. Uygun tarama araçları ve güvenilir kaynaklardan edinilen teknik açıklıklara ilişkin bilgiler (güvenlik uyarıları, sistem yamaları, virüs güncellemeleri vb), riskleri azaltmak için kullanılacaktır.

Önemli uygulamalar (özellikle Internete bağlı olanlar) ve ağ cihazları için sızma testleri, yürürlükteki yasa ve yönetmeliklere uygun olarak, yetkili üçüncü parti sağlayıcıları tarafından gerçekleştirilecektir.

10. BİLGİ GÜVENLİŞİ OLAY YÖNETİMİ

10.1 Bilgi Güvenliği Olaylarının ve Zayıflıklarının Raporlanması

Amaç: Bilgi sistemleri ile ilgili güvenlik olayları ve zayıflıkların, düzeltici önlemlerin alınması amacıyla, zamanında iletilmesi.

Politika: Tüm bilgi güvenliği olayları çalışanlarımız ve tedarikçi ve üçüncü parti kullanıcıları tarafından uygun yönetim kanalları ile mümkün olduğunca çabuk raporlanacaktır.

10.2 Bilgi Güvenliği Olayları ve İyileştirmelerinin Yönetimi

Amaç: Bilgi güvenliği olaylarının yönetiminde tutarlı ve etkili bir yaklaşımın uygulandığından emin olunması.

Politika: Bilgi güvenliğine ilişkin tüm olaylar (önem derecesinden bağımsız olarak) dokümante edilecek ve söz konusu olaylara ilgili müdür tarafından, Bilgi Güvenliği Koordinatörü aracılığı ile, müdahale edilecektir. Bilgi Güvenliği Koordinatörü söz konusu olayı, kök nedenin giderilmesine ve olayın yeniden ortaya çıkmasının önlenebilmesine olanak sağlamak amacıyla, Risk Yönetimi Birimi'ne en kısa sürede raporlayacaktır. Bilgi Teknolojileri Müdürlüğü söz konusu olayı, gerekli hallerde, aksiyon alınmak üzere daha üst mercilere iletebilecektir.

Meydana gelen bilgi güvenliği olayının bir varlığın gizlilik, bütünlük veya kullanılabilirlik özelliklerini tehlikeye atması halinde, varlığın sorumluluğunu taşıyan departman olayla ilgili bilgilendirilecek ve olayın tekrar ortaya çıkmasını engellemeye yönelik aksiyonlar alacaktır.

11. İŞ SÜREKLİLİŞİ YÖNETİMİ

11.1 İş Sürekliliği Yönetiminin Bilgi Güvenliği Açısı

Amaç: İş faaliyetlerindeki kesintilerin önlenmesi, bilgi sistemlerinin başlıca arızalarından veya felaketlerden etkilenen kritik iş süreçlerinin korunması ve tekrar makul bir zaman içerisinde yeniden işlerlik kazanmalarının sağlanması.

Politika: Önleyici ve kurtarıcı kontrollerin kombinasyonu kullanılarak, felaketlerin ve güvenlik hatalarının (doğal afetler, kazalar, ekipman arızaları ve kasıtlı eylemlerin sonucu gibi) yol açtığı

kesintileri kabul edilebilir bir seviyeye indirmeye yönelik bir iş sürekliliği yönetim süreci hayata geçirilecektir.

Acil durum planlamaları ve felaket kurtarma prosedürleri sadece bilgi sistemleri ile sınırlandırılmayacaktır.

Felaketlerin, güvenlik hatalarının ve hizmet kesintilerinin sonuçları analiz edilecektir. İş süreçlerinin gerekli zaman zarfı içinde yeniden işletilebilir hale getirilebilmeleri için, acil durum planları geliştirilecek ve hayata geçirilecektir. Söz konusu planlar sürekli olarak güncellenecek ve diğer yönetim süreçlerinin ayrılmaz bir parçası haline gelecektir. İş sürekliliği yönetimi, işlerin devamlılığına yönelik riskleri tespit edecek ve azaltacak kontrolleri kapsayacak, zarar verici olayların etkilerini sınırlayacak ve elzem iş süreçlerinin zamanında yeniden çalışır hale getirilmelerini sağlayacak şekilde tasarlanacaktır.

İş sürekliliği planları Yönetim Kurulu tarafından onaylanacak ve güncel ve etkili kalmalarının sağlanması amacıyla düzenli olarak test edilecek ve güncellenecektir.

12. UYUM

12.1 Yasal Gerekliliklere Uyum

Amaç: Herhangi bir yasal, düzenleyici veya sözleşmesel hükmün veya güvenlik gereksiniminin ihlalinden kaçınılması.

Politika: Bilgi sistemlerinin tasarımı, işletilmesi, kullanımı ve yönetimi süreçleri yasal, düzenleyici ve sözleşmeden doğan gereksinimlere tabi olabilecektir. Şirketimiz, bilgi güvenliğine ilişkin tüm yasal gerekliliklerin takip edilmesi ve söz konusu gerekliliklere uyulmasını sağlamaya yönelik düzenlemeler oluşturacaktır.

Belirli yasal gereksinimler konusunda destek, Şirket'in İç Kontrol ve Uyum Başkanlığı veya yetkin üçüncü parti hukuk danışmanlarından sağlanacaktır.

13. TEKNİK UYUM

Amaç: Bilgi sistemlerinin kurumsal güvenlik politikaları ve standartlarına uyumlu olmasının sağlanması.

Politika: Bilgi sistemlerinin güvenliği düzenli olarak gözden geçirilecektir. Bilgi sistemlerinin, düzenli incelemeler yoluyla, güvenlik politikaları ve güvenlik uygulama standartları ile uyumluluğu kontrol edilecektir.

Yöneticiler, kendi sorumluluk alanları içindeki tüm güvenlik prosedürlerinin doğru bir şekilde yürütülmesini sağlayacaklardır.

14. DOKÜMAN KONTROLÜ

Bu politikanın hazırlanması ve güncel tutulmasından Risk Yönetimi Birimi sorumludur.

Versiyon	Tarih	Onaylayan
1.0		