Halk Elektronik Para ve Ödeme Hizmetleri Anonim Şirketi

1. AMAÇ VE KAPSAM

Bu politikanın amacı, Halk Elektronik Para ve Ödeme Hizmetleri Anonim Şirketi'nin (bundan sonra "Şirket" olarak anılacaktır.) bilgi varlıklarını içeriden veya dışarıdan, planlı veya plansız meydana gelen tüm tehditlerden korumak, bilginin güvenli bir şekilde tutulmasını, transferini ve kullanılmasını sağlamaktır. Bilginin iş ihtiyaçlarına uygun kapsam ve yetkilendirme çerçevesinde kullanımını, personel ve tedarikçi çalışanlarının bilginin korunması ve kullanılması konusundaki rol ve sorumluluklarını belirtmek, bilgiye erişilebilirlik kapsamında iş sürekliliğini sağlamak ve beklenmedik durumların işe etkisini sınırlandırmak, Şirket'in yasal sorumlulukları doğrultusunda bilginin uygunsuz şekilde kullanımını engellemek, Şirket yöneticilerinin kendi iş alanlarında politikanın hayata geçirilmesinden ve personelinin de bu politikaya uygun hareket etmesinin sağlanmasından sorumlu olmasını temin etmektir.

2. KAPSAM

Bu doküman Şirket için çerçeve niteliğindeki, üst düzey bilgi güvenliği politikalarını belirlemek üzere hazırlanmıştır. Politika, Şirket'in tüm hizmet birimlerindeki bilgi sistemleri varlıklarını kapsar. Bilgi Güvenliği Politikası bilginin sözlü, yazılı, basılı, görsel vb. tüm formlarını kapsamakla beraber, Şirket'in bilgi varlıklarına erişen tüm personel ve tedarikçi çalışanları için geçerlidir.

3. SORUMLULUKLAR VE ROLLER

3.1. Yönetim Kurulu

Şirket bünyesinde bilgi güvenliğinin sağlanmasında nihai sorumluluk yönetim kuruluna aittir. Yönetim kurulu, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılığı göstermekle ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmekle yükümlüdür. Bu sorumluluk kapsamında yönetim kurulu, Şirket genelinde uygulanmasını gözetmekle yükümlü olduğu bir bilgi güvenliği yönetim sistemi tesis eder. Bilgi güvenliği politikasını onaylar.

3.2. Üst Yönetim

Üst yönetim, bilgi güvenliğinin sağlanması için gerekli organizasyonu, kaynakları ve

teknolojik altyapının tesisini sağlamaktadır. Bu yapıların, Şirket'in stratejik iş hedeflerine ve yasal mevzuata uygun şekilde bilgi güvenliği yönetimini gerçekleştirmesini gözetirler. Bilgi güvenliğinin kritik olduğu iş kararları alınırken, Bilgi Güvenliği Yöneticisinin tavsiyeleri dikkate alınır ve değerlendirilir. Bu sayede, Şirketin bilgi varlıklarını korumak ve güvenliğini sağlamak adına etkin bir stratejik yaklaşım benimsenmiş olur.

3.3. Bilgi Teknolojileri Genel Müdür Yardımcısı

Bilgi Teknolojileri Genel Müdür Yardımcısı, Bilgi Güvenliği ekibinin koordinasyonunu üstlenir ve bilgi güvenliği politikası, prosedürleri ve süreç dokümanlarının oluşturulması, güncellenmesi, onaya sunulması ve duyurulmasını sağlar. Ayrıca, bilgi varlıklarının sınıflandırılması ve BT risk yönetimi çalışmalarına aktif katkıda bulunarak gizlilik, bütünlük ve erişilebilirlik kriterleri açısından bilgi güvenliğini yönetir. İlgili birimlerle iş birliği yaparak iş gereksinimleri ve hedeflerine uygun şekilde Şirket genelinde bilgi güvenliğinin sağlanmasını destekler. Ayrıca, mevzuata, standartlara ve politika belgelerine uyumu takip eder, bilgi güvenliği faaliyetlerini yürütür ve testlerini gerçekleştirir. Önemli projeler ve değişiklikler için bilgi güvenliği gereksinimlerini belirlemede rol alır ve Şirket'in ilgili taraflarına yönelik bilgi güvenliği farkındalık programlarını yönetir. Son olarak, bilgi güvenliği istisnalarının onaylanmasını sağlar.

3.4. Bilgi Güvenliği ve Uyum Bölüm Müdürü

Bilgi Güvenliği ve Uyum Bölüm Müdürü, bilgi sistemlerinin geliştirilmesi, yönetimi ve işletimi için kullanılan teknolojilerin Şirket'in ihtiyaçlarına uygun şekilde uyarlanmasını sağlar. Bu kapsamda, BT süreçlerinin düzenlenmesi ve sağlıklı işleyişi için gerekli kontrollerin kurulması ve sürdürülmesiyle gizlilik, bütünlük ve erişilebilirlik ilkelerini gözetir. Ayrıca, bilgi sistemleri ve teknik hizmetlerin yönetimi sürecinde, Yönetim Kurulu tarafından onaylanmış olan Bilgi Güvenliği Politikası ve ilgili dokümanlara uyumun sağlanmasını temin eder. Bu şekilde, iş ihtiyaçlarını karşılarken güvenlik standartlarının ve politikalarının etkin bir şekilde uygulanmasını sağlar.

3.5. İş Birimi Yöneticileri

İş birimleri yöneticileri, kendi birimlerine ait verilerin belirlenmesi ve sahiplenmesinden sorumludur. Sahip oldukları verileri, gizlilik, kullanılabilirlik ve bütünlük gibi önemli kriterlere göre sınıflandırırlar. Sınıflandırılmış verilere ilişkin güvenlik kontrollerinin belirlenmesinde, bilgi güvenliği ekipleri ile koordineli bir şekilde çalışırlar.

3.6. İç Kontrol ve Denetim Bölüm Müdürlüğü

İç Kontrol ve Denetim Bölüm Müdürü Şirket içinde bilgi güvenliği yönetiminin sağlanmasına yönelik denetimleri, geçerli denetim standartlarına uygun olarak gerçekleştirir. Bu kapsamda, bilgi güvenliği süreçlerinin etkinliğini ve uyumluluğunu değerlendirerek gereken iyileştirmeleri belirler. Bu denetimler, bilgi güvenliği politikalarının, prosedürlerinin ve süreçlerinin etkin bir şekilde uygulanmasını sağlamak için önemli bir rol oynar.

3.7. İnsan Kaynakları, Organizasyon ve Performans Yönetimi Bölüm Müdürlüğü

İnsan Kaynakları Yönetimi, bilgi güvenliği farkındalığının oluşmasında, güvenlik politikasının ve bilgi güvenliği taahhütnamesinin kabul edilmesi sürecinde etkin rol alır. Bilgi sistemleri kaynaklarının uygun kullanımı kültürünün Şirket içinde gelişmesinde, uygunsuz kullanımların takip edilmesinde ve yeni personelin güvenlik taramasının yapılmasında bilgi güvenliği ekipleriyle beraber çalışır.

3.8. Personel ve Tedarikçi Çalışanları

Personel ve tedarikçi çalışanlar, politikaların, talimatların ve uygulamaların hükümlerine uygun hareket etmekten sorumludur. Bu kapsamda, işyerinde belirlenen kurallara ve yönergelerine uyum sağlamak, iş süreçlerinin doğru şekilde yürütülmesini sağlamak ve kurumun amaçlarına hizmet etmekle yükümlüdürler. Ayrıca, etik kurallara ve iş etiğine uygun davranışlar sergilemek de bu sorumlulukların bir parçasıdır. Personel ve tedarikçi çalışanlar, görevlerini yerine getirirken kurumun itibarını korumak ve güçlendirmek için çaba göstermelidirler.

4. POLİTİKA İLKELERİ

4.1. Bilgi Güvenliği Risk Yönetimi

Bilgi güvenliği riskleri, Kurumsal Risk Yönetimi süreci prosedürlerine uygun olarak yönetilir. Bu kapsamda, risklerin belirlenmesi, analiz edilmesi, değerlendirilmesi ve uygun risk yönetim stratejilerinin belirlenmesi adımları titizlikle izlenir. Böylelikle, Şirketin bilgi güvenliği alanında karşılaşabileceği riskler önceden tanımlanır ve etkin önlemler alınarak yönetilir. Bu süreç, bilgi varlıklarının korunması ve iş sürekliliğinin sağlanması açısından hayati öneme sahiptir.

4.2. Erişim Kontrolü

Erişim kontrolü, bilgi sistemlerinde her müşteri, personel ve tedarikçi çalışan için, inkâr edilemezlik, sorumluluk atama ve görevler ayrılığı prensiplerine dikkat edilerek gerekli en düşük yetkide bir kullanıcı hesabı oluşturulmasıyla sağlanır. Bu kullanıcı hesabı aracılığıyla bilgi sistemlerine erişim, verinin kritikliğine uygun kimlik doğrulaması ve yetkilendirme işlemleriyle gerçekleştirilir. Her kullanıcı, kendisine özel bir parola belirler. Ayrıca, kritik olarak belirlenen müşteri, personel ve tedarikçi çalışanlar tarafından gerçekleştirilen finansal işlemlere ait izler elektronik ortamda kaydedilir, yasal sürelere uygun olarak saklanır ve gerektiğinde yasal olarak kullanılır. Kullanıcı hesaplarının oluşturulması, ihtiyaçlara göre değiştirilmesi ve kapatılması da sistemli bir şekilde yönetilir. Bu sayede, bilgi sistemlerine güvenli ve kontrollü bir erişim sağlanarak güvenlik riskleri en aza indirilir.

4.3. Bilgi Varlıkları

Bilgi varlıkları, tanımlanır, sahiplendirilir ve yasal ile idari mevzuat ile iş gereksinimlerine uygun olarak sınıflandırılır. Bu sınıflandırmaya göre, bilgi varlıklarının gizliliği ve bütünlüğü korunurken erişilebilirliği sağlanır. Belirlenen sınıfa uygun olarak, bilgi varlıklarının korunması için gerekli tedbirler alınır ve kabul edilebilir kullanım koşulları belirlenir. Tüm taraflar, belirlenen kullanım koşullarına uygun hareket ederek bilgi varlıklarının güvenliğini sağlar ve korur. Bu şekilde, bilgi varlıklarının uygun bir şekilde yönetilmesi ve korunması için sistematik bir yaklaşım benimsenmiş olur.

4.4. Uyumluluk

Şirket, yürüttüğü süreç ve işlemlerin mevzuata uygunluğunu sağlar. Ayrıca, Şirket içinde yaşanan bilgi güvenliği olaylarının, yasal olarak geçerli kanıtlar sağlayacak şekilde incelenebilmesi için gerekli yapılar ve kontroller oluşturulur. Bu sayede, hem iş süreçlerinin mevzuata uygunluğu sağlanır hem de olası bilgi güvenliği ihlallerinin etkin bir şekilde araştırılması ve gerektiğinde yasal mercilere sunulması için uygun bir altyapı sağlanmış olur.

4.5. Veri Paylaşımı

Elde edilen veriler, edinim amacı dışında kullanılamaz. Sıfat ve görevleri dolayısıyla Şirket veya müşterilerine ait sırları öğrenenler, söz konusu sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Bu yükümlülük görevden ayrıldıktan sonra da devam eder. Yasal uyum otoritelerinin istekleri ve kanuni soruşturmalar kapsamında talep edilen verilerin, sistemlerden mevcut yapılarla alınamaması durumunda, ilgili veriler BT personeli tarafından hazırlanacak amaca özel sorgu, programlama gibi yöntemlerle ilgili işlem kayıtlarından yararlanılarak oluşturulur. Verilerin paylaşımı, belirlenen kabul edilebilir kullanım koşullarına göre yapılır.

4.6. Bilgi Güvenliği Olay Yönetimi

Bilgi Güvenliği Olay Yönetimi, kurumun faaliyetlerini en az etkileyecek şekilde ve mümkün olan en kısa sürede bilgi sistemleri hizmetlerini normal işleyişine döndürmek amacıyla siber olayların ele alınması ve takibine yönelik bir süreç oluşturulur. Bu çerçevede, siber olaylara müdahale süreci belirlenir ve uygulanır. Bilgi güvenliği olaylarının incelenmesinde, kanıtların yasal olarak geçerli olmasını sağlayacak yöntemler kullanılır ve gerekli adımlar atılır. Ayrıca, personel ve tedarikçi çalışanları, fark ettikleri bilgi güvenliği olaylarını derhal bildirmekle yükümlüdürler. Bu sayede, olası güvenlik ihlalleri hızla tespit edilir ve uygun önlemler alınarak gereken müdahale yapılır.

4.7. İş Sürekliliği ve Olağan Üstü Durum

İş etki analizi sonucunda kritikliği belirlenen bilgi varlıkları için iş sürekliliği ve olağanüstü durum planları oluşturulur. Hazırlanan planlar düzenli olarak uygun

yöntemlerle test edilir ve güncellenir. Planların personel ve tedarikçi çalışanları tarafından öğrenilmesi için gerekli eğitimler sağlanır. Olağanüstü bir durum yaşanması durumunda, öncelikli olarak açılacak hizmetler ve hizmetlerin sağlanamamasına ilişkin tahammül edilebilecek süre ve veri kaybı miktarı belirlenir. Buna uygun olarak olağanüstü durum merkezi altyapısı sağlanır ve gerekli önlemler alınır. Bu sayede, iş sürekliliğinin sağlanması ve olağanüstü durumlarla etkin bir şekilde başa çıkılması için gereken altyapı ve planlamalar oluşturulmuş olur.

4.8. Fiziksel ve Çevresel Güvenlik

Fiziksel güvenlik kontrollerinde, insan hayatının güvenliği her zaman öncelikli olarak ele alınır. Bu çerçevede, veri merkezleri ve sistem odaları kritiklik seviyelerine göre çevresel tehditler ve doğal afetlere karşı güvenli hale getirilir. Bilgi varlıklarına fiziksel olarak erişimler, güvenlik sınıflarına uygun olarak kısıtlanır, izlenir ve güvenliği sağlanır. Böylelikle hem çalışanların hem de tesislerin güvenliği maksimum düzeyde korunur ve bilgi varlıklarının güvenliği sağlanmış olur.

4.9. Temiz Masa

Masa başından geçici olarak ayrılma, gün sonunda çalışma ortamından ayrılma veya uzun süreli çalışma ortamından ayrılma gibi durumlarda veriler, güvenlik sınıfına uygun şekilde saklanır ve kullanılır. Parolalar genel ilke olarak yazılı hale getirilmez; ancak iş gerekliliği sebebiyle yazılı olarak bulundurulması gerektiğinde yetkisiz erişimlere karşı önlemler alınır. Toplantılar sonrasında toplantı odasında yazı tahtasında veya masa üstünde bilgi bırakılmaz. Kullanım ömrü sona eren veya artık ihtiyaç duyulmadığına karar verilen bilgiler, kâğıt öğütücü, disk/disket yok edici gibi yöntemlerle imha edilir. Böylelikle, bilginin geri dönüşümünün veya yeniden kullanılabilir hale gelmesinin önüne geçilir ve güvenliğin korunması sağlanır.

4.10. Bilgi Sistemleri İşletimi ve İletişimi

Üretim ortamı dışındaki ortamlardaki bilgi sistemlerine, herhangi bir kısıtlama olmadan internet üzerinden erişime izin verilmez. Ancak üretim ortamında ihtiyaç duyulan bilgi sistemleri için güvenlik gereksinimlerine uygun şekilde internet erişim yetkisi sağlanır. Bilgi sistemlerinin iletişiminde, güncel ve güvenliğini yitirmemiş teknikler kullanılarak, verilerin korunması ve güvenliği sağlanır. Bu sayede hem üretim ortamındaki ihtiyaçlar karşılanır hem de bilgi sistemlerinin güvenliği

maksimum seviyede korunmuş olur.

4.11. Bilgi Sistemleri Edinimi Geliştirilmesi ve Bakımı

Bilgi sistemlerinin edinimi, geliştirilmesi veya bakımı süreçlerinde, bilgi güvenliği gereksinimlerine öncelikle yer verilir. Dış hizmet alımı kapsamındaki sistemlerin, süreçlerin ve hizmetlerin, yasal ve idari mevzuata uygun olmasının yanı sıra Şirket'in güvenlik politikasına da tam uyumluluğu sağlanır. Bu sayede, dış hizmet alımlarında da güvenlik standartlarından ödün verilmez ve Şirketin bilgi varlıkları maksimum düzeyde korunmuş olur.

4.12. Bilgi Güvenliği Farkındalığı

Bilgi sistemleri kullanıcılarına yönelik bilgilendirme ve eğitim çalışmalarıyla bilgi güvenliği farkındalığı oluşturulur. Bu eğitimler, kişilerin rolleri ve sorumluluklarına uygun şekilde düzenlenir ve sunulur. Personele ve tedarikçi çalışanlarına düzenli olarak bilgi güvenliği farkındalığı ölçümleri yapılır ve gerekli iyileştirmeler uygulanır. İşe yeni alınan her personel ve tedarikçi çalışanı, bilgi güvenliği konusunda özel olarak bilgilendirilir ve eğitilir. Bu şekilde, çalışanların bilgi güvenliği konusundaki bilinç düzeyi artırılarak güvenli bir iş ortamı sağlanır.

4.13. Bilgi Sistemleri Etik ve Kabul Edilebilir Kullanımı

Bilgi sistemleri ve hizmetleri (İnternet, e-posta, telefon, faks, bilgisayarlar, mobil cihazlar ve cep telefonları dâhil olmak üzere), kurum işlerinin sağlıklı bir şekilde yürütülmesini sağlamak için kullanılır. Bu sistemlerin kullanımı sadece iş amaçları için yapılır; yasa dışı, rahatsız edici, Şirket'in diğer politika, standart ve rehberlerine aykırı veya kuruma zarar verebilecek şekilde kullanılmaz. Sağlanan internet, telefon veya e-posta gibi işe yönelik kullanılan bilgi sistemleri ve hizmetler, kişisel amaçlarla kullanılmaması için özen gösterilir. Personel ve tedarikçi çalışanları, sosyal medya profil ve paylaşımlarında, kurum kimliğine uygun şekilde hareket eder; Şirket, ortakları, diğer personel ve tedarikçi çalışanları ve müşterileri kötüleyici veya küçük düşürücü davranış ve paylaşımlardan kaçınır. Bu sayede, kurumun itibarı korunur ve profesyonel bir çalışma ortamı sürdürülür.

5. İSTİSNA SÜRECİ

Bilgi Güvenliği Alt Dokümanları kapsamında belirtilen herhangi bir hususa aykırı işlemlerin yapılması gerektiğinde, talep sahibi gerekli telafi edici kontrolleri göz önünde bulundurarak Bilgi Güvenliği ve Uyum Bölüm Müdürü' ne bilgi verir ve ilgili birimlerce kontrol istisnaları tanımlanır. Bu istisnaların Kurumsal Risk Yönetimi süreci içinde onaylanması gerekir ve riskin Bilgi Güvenliği stratejisine ve mevzuata uygun olması şarttır. Kabul edilecek bir riskin aynı zamanda bir iş süreci veya iş uygulamasıyla ilgili olması durumunda, ilgili iş biriminin üst düzey yöneticisinin de riskin kabul edildiğine dair onayı gereklidir. Bu şekilde, işleyişin şeffaflığı sağlanır ve uygun telafi edici önlemler alınarak risklerin kontrol altına alınması mümkün olur.

6. TANIM VE KISALTMALAR

Bilgi Varlığı, elektronik ve/veya fiziksel ortamlarda yer alan; ödeme hizmeti faaliyetlerinin yürütülmesinde kullanılan veriler ile bu verilerin taşındığı, saklandığı, iletildiği veya işlendiği sistem, yazılım, ağ cihazları, BT donanımları, iş süreçleri, bilgiyi kullanan ve taşıyan personel ile bilgiyi barındıran fiziksel mekânlar gibi Şirket için değeri olan varlığı ifade eder.

Bilgi Teknolojileri (BT), herhangi bir biçimdeki verinin, girişinin yapılması, saklanması, işlenmesi, iletilmesi ve çıktılarının alınması için kullanılan donanım, yazılım, iletişim altyapısı ve ilgili diğer teknolojilerdir.

Bilgi Sistemleri (BS), bilginin toplanması, işlenmesi, saklanması, dağıtımı ve kullanımına yönelik insan kaynağı, operasyonel faaliyetler ve süreçler ile bunlarla etkileşim içinde bulunan bilgi teknolojilerini belirtir.

Bilgi Güvenliği, iş sürekliliğini sağlamak, iş riskini en aza indirmek ve yatırımlar ile iş fırsatlarının getirisini azami seviyeye çıkartmak, yasal gerekliliklere uyum sağlamak, müşteri mahremiyetinin sağlanması, Şirket itibarının korunması gibi amaçlarla bilgilerin dış ve iç tehditlere karşı korunmasıdır.

Bilgi Güvenliği Olayı, iş faaliyetlerini riske atma ve bilgi güvenliğini tehlikeye düşürme olasılığı yüksek olan tek başına veya bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olaylarıdır.

Bilgi Güvenliği Ekipleri, Bilgi Güvenliği ve Uyum Bölüm Müdürlüğü personelini ifade etmektedir.

Bilgi Güvenliği Alt Dokümanları, bilgi güvenliği alt politikası, bilgi güvenliği standardı, bilgi güvenliği süreci, bilgi güvenliği prosedürü, bilgi güvenliği görüşü, bilgi güvenliği farkındalık eğitim programı, bilgi güvenliği sözleşmesi formatlarında hazırlanan dokümanları ifade eder.