Halk Elektronik Para ve Ödeme Hizmetleri Anonim Şirketi

1. AMAÇ

İşbu politika ile bilgi varlıklarını, içeriden veya dışarıdan, planlanmış veya istenmeden meydana gelen tüm tehditlerden korumak, bilginin güvenli bir şekilde tutulmasını, transferini ve kullanılmasını sağlamak, bilginin iş ihtiyaçlarına uygun kapsam ve yetkilendirme çerçevesinde kullanımını sağlamak, 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, Kuruluşumuzun yasal sorumlulukları doğrultusunda, bilginin uygunsuz şekilde kullanımını engellemek, Şirketimiz yöneticilerinin kendi iş alanlarında politikanın hayata geçirilmesinden ve personelinin de bu politikaya uygun hareket etmesinin sağlanmasından sorumlu olmasını temin etmek amaçlanmaktadır.

2. KAPSAM

İşbu doküman Halk Elektronik Para ve Ödeme Hizmetleri Anonim Şirketi (Bundan sonraki bölümlerde Şirket olarak ifade edilecektir.) 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, teknolojik altyapının tesisini sağlar. Bu yapıların bilgi güvenliği yönetimini Şirket'in stratejik iş hedeflerine ve yasal mevzuata uygun olarak yerine getirmesini gözetir. Bilgi güvenliğinin kritik olduğu iş kararları alınırken, Bilgi Güvenliği Komitesinin tavsiyelerini değerlendirir.

3.3. Bilgi Güvenliği Komitesi

Bilgi güvenliğinin tüm Şirket süreçlerinde, teknolojilerinde ve kurum çalışanlarının faaliyetlerinde uygulanmasını gözetecek olan iş birimlerinin üst yöneticilerinin, bilgi güvenliğinin sağlanması sürecinde etkin olabilmesi için bir Bilgi Güvenliği Komitesi oluşturulur. Bilgi Güvenliği Komitesi, bilgi güvenliğinin sağlanmasında ve kabul edilebilir risk seviyelerinin belirlenmesinde fikir birliği içinde olur. Bilgi güvenliğinin iş ihtiyaçları stratejilerine uygun olmasına ve Şirket kültüründe Kabul görmesine önderlik eder. Bilgi Güvenliği Komitesinin üyeleri, görev kapsamı, sorumlulukları ve yönergesi Bilgi Güvenliği Yöneticisi tarafından belirlenir ve güncellenir, Bilgi Teknolojileri Genel Müdür Yardımcısının uygun görüşü ve Yönetim Kurulu Makam Oluru ile yürürlüğe alınır.

3.4. Bilgi Teknolojileri Genel Müdür Yardımcısı

Bilgi Güvenliği ekibinin koordinasyonunu, bilgi güvenliği politikası, prosedürleri ve süreç dokümanlarının oluşturulmasını, bunların güncellenmesini, onaya sunulmasını ve duyurulmasını, bilgi güvenliği bakış açısıyla, bilgi varlıklarının sınıflandırılmasını ve bilgi varlıklarına yönelik gizlilik, bütünlük, erişilebilirlik kriterleri bakımından BT risk yönetimi çalışmalarına aktif katkı sunulmasını, ilgili birimlerle uyum içinde, iş gereksinimleri ve iş hedefleriyle uyumlu Şirket genelinde bilgi güvenliğinin tesis edilmesini, bilgi güvenliği ile ilgili mevzuat hükümlerine, standartlara, politika, prosedür ve süreç dokümanlarına uyumun takip edilmesini, bilgi güvenliği faaliyetlerinin ve testlerinin yürütülmesinin sağlanmasını ve bunların takip edilmesini, önemli projeler ve değişiklikler için bilgi güvenliği gereksinimlerinin belirlenmesi çalışmalarına katkıda bulunulmasını, Şirket'in bilgi güvenliğini ilgilendiren taraflara yönelik bilgi güvenliği farkındalık programının yürütülmesini, bilgi güvenliği istisnalarının onaylanmasını sağlar.

3.5. Bilgi Güvenliği ve Altyapı Birim Müdürü

Bilgi sistemlerinin geliştirilmesi, yönetimi, işletimi için kullanılan teknolojilerin Şirkete uyarlanması, buna yönelik BT süreçlerinin düzenlenmesi ve sağlıklı işleyişi için gerekli kontrollerin tesisinde gizlilik, bütünlük ve erişilebilirliğinin sağlanmasını gözetir. Bilgi sistemleri ve teknik hizmetler yönetiminin, iş ihtiyaçlarını karşılarken, Yönetim Kurulu tarafından onaylanmış Bilgi Güvenliği Politikasına ve Bilgi Güvenliği Alt Dokümanlarına uyumlu olacak şekilde yürütülmesini gözetir.

3.6. İş Birimi Yöneticileri

İş birimleri yöneticileri, birimlerine ait verileri belirler ve sahiplenir. Sahibi oldukları verileri gizliliğine, kullanılabilirliğine ve bütünlüğüne göre sınıflandırır. Sınıflandırılmış verilere uygulanacak güvenlik kontrollerinin belirlenmesinde, bilgi güvenliği ekipleri ile koordineli olarak çalışırlar. Bilgi güvenliği açısından kritik iş birimlerinin yöneticileri Bilgi Güvenliği Komitesinde temsil edilir.

3.7. İç Denetim ve Uyum Birim Müdürlüğü

İç Denetim ve Uyum Birimi olarak, Şirket içinde bilgi güvenliği yönetiminin sağlanmasına yönelik denetimleri, geçerli denetim standartlarına uygun olarak gerçekleştirir. Bilgi Güvenliği Komitesinde temsil edilir.

3.8. İnsan Kaynakları, Organizasyon ve İdari İşler Birim 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. İnsan Kaynakları, Organizasyon ve İdari İşler Birim Müdürlüğü Bilgi Güvenliği Komitesinde temsil edilir.

3.9. Personel ve Tedarikçi Çalışanları

Politikaların, talimatların ve uygulamaların hükümlerine uygun hareket etmekten sorumludur.

4. POLİTİKA İLKELERİ

4.1. Bilgi Güvenliği Risk Yönetimi

Bilgi güvenliği riskleri, Kurumsal Risk Yönetimi süreci prosedürlerine uygun olarak yönetilir.

4.2. Erişim Kontrolü

Bilgi sistemleri üzerinde, her müşteri, personel ve tedarikçi çalışanı için, inkâr edilemezlik, sorumluluk atama, görevler ayrılığı prensibi dikkate alınarak gerekli en düşük yetkide iş ihtiyacına uygun bir kullanıcı hesabı oluşturulur. Bu kullanıcı hesabı ile bilgi sistemlerine erişim, verinin kritikliğine uygun kimlik doğrulaması ve yetkilendirme ile gerçekleştirilir. Her kullanıcının kendisine özel parolası olur. Kritik olarak belirlenmiş olan müşteri ve personelin veya tedarikçi çalışanlarının gerçekleştirdiği finansal işlemlere ait izler elektronik ortamda kaydedilir, yasal sürelere uygun olarak saklanır, yasal olarak gerekmesi durumunda kullanılır. Kullanıcı hesaplarının oluşturulması, ihtiyaçlara göre değiştirilmesi ve kapatılması sağlanır.

4.3. Bilgi Varlıkları

Bilgi varlıkları, tanımlanır, sahiplendirilir, yasal ve idari mevzuat ile iş gereksinimlerine uygun sınıflandırılır. Yapılan sınıflandırmaya göre bilgi varlıklarının gizliliği ve bütünlüğü korunur, erişilebilirliği sağlanır. Bilgi varlığının belirlenen sınıfına uygun tedbirler alınır ve kabul edilebilir kullanım koşulları belirlenerek tüm taraflarca buna uygun hareket edilir.

4.4. Uyumluluk

Şirket, yürüttüğü süreç ve işlemlerin mevzuata uygun olmasını sağlar. Şirket içinde yaşanan bilgi güvenliği olaylarının, yasal olarak geçerli kanıtlar sağlayacak şekilde incelenebilmesi için gerekli yapılar ve kontroller tesis edilir.

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

Siber olaylardan sonra kurum faaliyetlerini en az etkileyecek şekilde ve mümkün olan en kısa sürede bilgi sistemleri hizmetlerini normal işleyişine döndürmek üzere gerçekleşen siber olayların ele alınmasına ve takibine yönelik siber olay yönetimi ve siber olaylara müdahale süreci oluşturulur. Bilgi güvenliği olaylarının incelenmesinde, kanıtların yasal olarak geçerli olmasını sağlayacak yöntemler kullanılır. Personel ve tedarikçi çalışanları, fark ettikleri bilgi güvenliği olaylarını bildirmekle yükümlüdür.

4.7. İş Sürekliliği ve Olağan Üstü Durum

İş etki analizi sonucunda kritikliği belirlenen bilgi varlıkları için iş sürekliliği ve olağan üstü durum planları oluşturulur. Hazırlanan planlar düzenli olarak uygun yöntemlerle test edilir. Planların personel ve tedarikçi çalışanları tarafından öğrenilmesi sağlanır. Olağanüstü bir durum yaşanması durumunda öncelikli olarak açılacak hizmetler ve hizmetlerin sağlanamamasına ilişkin tahammül edilebilecek süre ve veri kaybı miktarı belirlenir, buna uygun olağanüstü durum merkezi altyapısı sağlanır.

4.8. Fiziksel ve Çevresel Güvenlik

Fiziksel güvenlikte sağlanacak tüm kontrollerde insan hayatının güvenliği öncelikli olarak ele alınır. 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.

4.9. Temiz Masa

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

4.10. Bilgi Sistemleri İşletimi ve İletişimi

Üretim ortamı haricindeki ortamlardaki bilgi sistemleri herhangi bir kısıtlama olmadan internet üzerinden erişime açılamaz. Üretim ortamında ihtiyaç duyulan bilgi sistemleri için güvenlik gereksinimlerine uygun şekilde internet erişim yetkisi verilir. Bilgi sistemlerinin iletişiminde güncel, güvenliğini yitirmemiş teknikler kullanılır.

4.11. Bilgi Sistemleri Edinimi Geliştirmesi ve Bakımı

Bilgi sistemlerinin edinimi, geliştirilmesi ya da bakımı süreçlerinde, bilgi güvenliği gereksinimlerine yer verilir. Dış hizmet alımı kapsamındaki sistem, süreç ve hizmetlerin, yasal ve idari mevzuata yanı sıra Şirket'in işbu güvenlik politikasına uygun olması sağlanır.

4.12. Bilgi Güvenliği Farkındalığı

Bilgi sistemleri kullanıcılarına yönelik bilgilendirme ve eğitim çalışmalarıyla farkındalık yaratılır. Bilgi güvenliği eğitimleri, kişilerin rol ve sorumluluklarına uygun olur. Personele ve tedarikçi çalışanlarına yönelik düzenli olarak bilgi güvenliği farkındalığı ölçülür. İşe yeni alınan her personel ve tedarikçi çalışanı bilgi güvenliği konusunda bilgilendirilir.

4.13. Bilgi Sistemleri Etik ve Kabul Edilebilir Kullanımı

Bilgi sistemleri ve hizmetleri (İnternet, e-posta, telefon, faks, bilgisayarlar, mobil cihazlar ve cep telefonları da dâhil olmak üzere) kurum işlerinin sağlıklı bir şekilde yürütülmesini sağlamak için kullanılır. Bu sistemler, iş amaçları dışında, yasa dışı, rahatsız edici, Şirket'in diğer politika, standart ve rehberlerine aykırı veya kuruma zarar verecek herhangi bir şekilde kullanılmaz. Sağlanan internet, telefon veya e-posta adresi gibi işe yönelik kullanılan bilgi sistemleri ve hizmetlerin kişisel amaçlarla kullanılmaması konusunda azami özen gösterilir. Personel ve tedarikçi çalışanları, sosyal medya profil ve paylaşımlarında, kurum kimliğine uygun düşmeyecek şekilde hareket etmez; Şirketi, ortaklarını, diğer personel ve tedarikçi çalışanlarını ve müşterileri kötüleyici ve küçük düşürücü davranış ve paylaşımlarda bulunmaz.

5. İSTİSNA SÜRECİ

Bilgi Güvenliği Alt Dokümanları kapsamında yer verilen herhangi bir hususa aykırı işlemlerin yapılması gerektiğinde, talep sahibi tarafından gerekli telafi edici kontroller göz önüne alınarak uygulanacak adımlar hakkında Bilgi Güvenliği ve Altyapı Birim Müdürüne bilgi verilir ve ilgili birimlerce kontrol istisnaları

tanımlanır. İstisnalar Kurumsal Risk Yönetimi süreci kapsamında onaylanır. Riskin BS stratejisine ve mevzuata aykırılık teşkil etmemesi şarttır. Kabul edilecek riskin aynı zamanda bir iş süreci veya iş uygulamasıyla ilgili olması durumunda ilgili iş biriminin üst düzey yöneticisinin de riskin kabul edildiğine ilişkin onayının bulunması gerekir.

6. TANIM VERİ 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 Sistemleri BT Bölüm Müdürlüğü ile birlikte Bilgi Sistemleri Güvenlik Ofisini 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.