A ÖDEME VE ELEKTRONİK PARA HİZMETLERİ A.Ş.

Bilgi Güvenliği Politikası

Doküman No	POL.01
Doküman Adı	Bilgi Güvenliği Politikası
Versiyon	V.3.0
Güncelleme	03.01.2025

İçindekiler

1. Amaç ve Kapsam

1. Politikanın amacı bilgi sistemlerinin ve üzerinde işlenmek, iletilmek, depolanmak ve yedek olarak saklanmak üzere bulunan verilerin gizlilik, bütünlük ve ulaşılabilirliklerini sağlayacak önlemlere ilişkin kontrol altyapısını geliştirilmek ve düzenli olarak güncellenmesine yönelik kural ve kontrolleri belirlemektir.
2. A Ödeme bilgi sistemleri ve üzerinde işlenen, iletilen, depolanan ve yedek olarak saklanan tüm varlıkları kapsamaktadır.
3. Politika aynı zamanda, Kuruluş bilgi sistemleri altyapısını kullanmakta olan tüm personeli, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

2. Dayanak

4. Bu prosedür, Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ'in 8 inci maddesi kapsamında hazırlanmıştır.

3. Tanımlar

Banka: Türkiye Cumhuriyet Merkez Bankası

Bilgi sistemleri: Ödeme hizmetine ilişkin faaliyetlerin yürütülmesi amacıyla ödeme hizmeti sağlayıcısının bilgi ve verilerle ilgili olarak mevzuatla belirlenmiş sorumluluklarının yerine getirilmesini sağlayan donanım, yazılım, veri, süreç ve insan kaynağından oluşan yapının tamamı

BT: Bilgi Teknolojileri

BT Bölümü: Bilgi Teknolojileri Bölümü

Denetim izi: Bir finansal ya da operasyonel işlemin başlangıcından bitimine kadar takip edilmesini sağlayacak kayıtlar

Kimlik Doğrulama: Bildirilen bir kimliğin gerçekten bildiren kişiye ait olduğuna dair güvence sağlayan mekanizma

Kurum: A Ödeme ve Elektronik Para Hizmetleri A.Ş.

Taşınabilir Aygıtlar: Dizüstü bilgisayarlar, akıllı telefonlar, tablet bilgisayarlar, CD,

DVD, USB hafıza cihazları ve Hard disk sürücüleri

Şifreleme Açık Anahtarı: Açık anahtarlı şifrelemede kullanılan, herkesin erişimine ve kullanımına açık olan, şifreleme gizli anahtarı ile matematiksel bağlantısı bulunan ve şifreleme gizli anahtarı ile atılan imzayı kontrol etmek, yapılan şifrelemeyi çözmek, ya da sadece şifreleme gizli anahtarının çözebileceği şekilde verinin şifrelenmesi için kullanılan şifreleme anahtarı

Şifreleme Gizli Anahtarı: Açık anahtarlı şifrelemede imza atma, şifreleme ve karşılığı olan şifreleme açık anahtarıyla şifrelenmiş veriyi çözmek için kullanılan, sadece sahibi tarafından bilinmesi ve kullanılması gereken anahtar

Şifreleme Anahtarı: Şifreleme algoritmasının şifreleme ve şifre çözme amacıyla kullanıldığı karakter dizini

SSL (Secure Socket Layer): İnternet üzerinde bilginin gizliliğini ve bütünlüğünü korumak için oluşturulmuş bir protokol katmanıdır. Bu protokol bütün yaygın web sunucuları ve tarayıcıları tarafından desteklenmektedir. Bu protokolle çalışan web siteleri ‘http’ yerine ‘https’ ile başlar. SSL, gönderilen bilginin sadece doğru adreste deşifre edilmesini sağlar; bilgi gönderilmeden önce şifrelenir ve sadece doğru alıcı tarafından deşifre edilir. Bilginin bütünlüğü de bu süreçte kontrol edilir.

Tebliğ: Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin

4. Sorumluluklar

4.1. BT Bölümü

5. Güvenlik olay yönetimi sürecinin prosedüre uygun olarak işletildiğini kontrol etmek, izlemek ve raporlamak
6. Bilgi Güvenliği Politikasının oluşturulması, uygulanması ve güncelliğinin sağlanması
7. Bilgi Güvenliği Politikasının sağlanması amacıyla teknoloji altyapısı, süreçler ve insan kaynağı konusunda kaynak planlamasının yapılması
8. Risk Envanteri kapsamında BT risklerinin belirlenmesi, yönetilmesi ve Risk Yönetimi sorumlusu ile koordineli olarak güncelliğinin sağlanması
9. Bilgi sistemleri üzerinde etkin ve yeterli iç kontrollerin tesis edilmesi

10. Güvenlik kontrol sürecini değerlendirmeye tabi tutulması ve uygunluğunun onaylanması
11. Veri Sınıflandırma çalışmasının gerçekleştirilmesi ve güncelliğinin sağlanması
12. İç güvenlik testleri ile bağımsız sızma testlerinin gerçekleştirilmesi sürecinin koordine edilmesi, aksiyonların planlaması, uygulanması, sonuçların raporlanması ve kontroller ile oluşturulan yapıların teknolojik gelişmelere göre güncellenmesi
13. Bilgi güvenliği olaylarına yönelik incelemenin yapılabilmesi için kritik sistem ve veri tabanları için denetim izlerini kaydederek yasal gerekliliklere uygun süreler içerisinde saklanması
14. A Ödeme çalışanlarının bilgi güvenliğine ilişkin farkındalıklarının arttırılması amacıyla faaliyetlerde bulunulması ve periyodik olarak bilgi güvenliği farkındalık eğitimlerinin düzenlenmesi
15. A Ödeme Bilgi Güvenliği Politikasının tüm çalışanlara duyurulması ve bilgi güvenliğine ilişkin taahhütnamelerin tüm çalışanlar tarafından imzalanması süreçlerinin tesis edilmesi
16. Bilgi güvenliğine ait ihlallerin izlenmesi, raporlanması ve aksiyon planlarının oluşturulması, Bilgi güvenliği olaylarının izlenmesi ve periyodik olarak değerlendirilmesi
17. Bilgi Güvenliği Planı'nın hazırlanması ve onaylanması
18. Bilgi kaynaklarına yönelik tehditlerin periyodik olarak değerlendirilmesi
19. Kullanıcı Kimlik ve Hesap Yönetimi standartlarının belirlenmesi

4.2. Kurum Personeli

20. Bilgi Güvenliği Politikası ve politika ile ilgili tüm prosedürlere uyulması
21. Sahibi olduğu veriler için sınıflandırma çalışmasının gerçekleştirilmesi
22. Veri sınıflandırma çalışması sonucu belirlenen güvenlik kontrollerine uyulması
23. Bilgi güvenliğine yönelik tespit edilen olayların ivedilikle BT Müdürü'ne bildirilmesi
24. A Ödeme kaynaklarına erişim için kullanılan her türlü hesap/parola bilgisinin saklı tutulması ve BT personeli dahil hiç kimseyle paylaşılmaması

5. Genel Esaslar

25. Bilgi güvenliği altyapısı ve organizasyonu, Kurumun bilgi güvenliğine ilişkin temel ilkeleri ve bu konudaki mevzuat yükümlülükleri baz alınarak uygulanır ve geliştirilir.

26. İş birimlerinin bilgi ihtiyaçları, BT konfigürasyonu, bilgi risk aksiyon planları ve bilgi güvenliği kültürü genel bir BT güvenlik planına dönüştürülmektedir.

27. Plan; hizmetler, personel, yazılım ve donanıma yapılacak uygun yatırımlarla beraber güvenlik politika ve prosedürlerinde uygulanmaktadır. BT Sorumlusu tarafından plan yıllık olarak hazırlanmakta ve üst yönetim onayına sunulmaktadır.

28. A Ödeme, bilgi güvenliği yönetim süreci kapsamında, bilgi sistemleri aracılığıyla sunduğu hizmetlerin tasarımı, geliştirilmesi, uygulanması veya yürütülmesinde görevi bulunmayan bağımsız ekiplere yılda en az bir defa sızma testi yaptırılmakta ve sonuçlarına göre gerekli aksiyonlar alınmaktadır.

29. Bilgi Güvenliği Politikasının hazırlanması ve güncelliğinin sağlanması, politikanın uygulanması amacıyla kaynak ayırmak ve karar almak BT Sorumlu'sunun sorumluluğundadır.

6. Bilgi Güvenliği Politikası Standartları

6.1. Veri Sınıflandırma Süreci

30. Bilgi sistemleri ve bilgi sistemleri üzerinde işlenen, iletilen, depolanan ve yedek olarak tutulan veriler güvenlik hassasiyet derecelerine göre sınıflanır, her bir sınıf için uygun düzeyde güvenlik kontrolleri tesis edilir.

31. Bu konu ile ilgili işleyiş ve sorumluluklar "Veri Sınıflandırma Prosedürü" doğrultusunda düzenlenmektedir.

32. Tüm A Ödeme çalışanları ve ilgili verilere erişen üçüncü parti firma çalışanları "Veri Sınıflandırma Prosedürü" doğrultusunda veri ve veri sınıfları için belirlenen güvenlik, gizlilik, erişim, iletim vb. kontrollerine uymak ile yükümlüdürler.

6.2. Risk Belirleme ve Değerlendirme Süreci

33. Bilgi sistemleri ve içerdiği verilerin güvenliği konusunda gerekli kontrollerin ve yapıların oluşturulması çalışmaları kapsamında; BT risk tespiti ve risk değerlemesi yapılması "Risk Yönetimi Politikası" ve "Bilgi Sistemleri Risk Yönetimi Prosedürü" doğrultusunda gerçekleştirilmektedir.

34. BT risklerinin belirlenmesi ve değerlendirilmesi sürecinin işletilmesi BT sorumluluğunda olup, risklerin doğru olarak değerlendirildiğinin incelenmesi, onaylanması ve risk aksiyonlarının takip edilmesi Risk Yönetimi ekibinin sorumluluğundadır.

6.3. Bilgi Güvenliği Farkındalık Süreci

35. A Ödeme personelinin güvenlik konusunda farkındalık kazanmaları amacıyla her sene periyodik olarak Bilgi Güvenliği Farkındalık Eğitimleri düzenlenir.
36. Bilgi Güvenliği Farkındalık eğitimlerine katılım tüm personel ve temsilciler için zorunlu olup gerek duyulduğu hallerde A Ödeme ile çalışan üçüncü parti firma personelinin de eğitime katılımları talep edilebilir.
37. Eğitime katılıma ilişkin eğitim katılım formu düzenlenir. Eğitim içeriği her sene gözden geçirilerek değişiklik ihtiyacı tespit edilen durumlarda güncellenir.

6.4. Görevler Ayrılığı Prensibi

38. Bilgi sistemlerine ilişkin sistem, veri tabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde görevler ayrılığı prensibi uygulanır, atanan görevler ve sorumluluklar görevler ayrılığı prensibine göre periyodik olarak gözden geçirilir ve gerekiyorsa güncellenir.
39. Süreçler ve sistemler, kritik bir işlemin tek bir personel veya tedarikçi firma tarafından girilmesi, yetkilendirilmesi ve tamamlanmasına imkân vermeyecek şekilde tasarlanır.
40. Uygulama, veri tabanı ve işletim sistemi seviyesinde yetkilendirme yapılırken aşağıdaki görevler ayrılığı standartlarına uygun yetkilendirme yapılır:
41. Aktif dizin yöneticisi (domain admin) rolü ilgili BT personeline atanır ve aktif dizin yöneticisi haricindeki personele sistem yöneticisi (domain admin) yetkisi verilmez.
42. Yüksek yetkili yönetici hesapları rolü ilgili BT personeline atanır ve bu personel haricindeki personele sistem yöneticisi yetkisi verilmez.
43. Dış hizmet alımına konu sözleşme kapsamında veri tabanında sınırsız yetkiye sahip olan ve veri tabanının yönetiminden sorumlu personel rolü ilgili tedarikçi personeline atanır ve bu personel haricindeki personele veri tabanına doğrudan sınırsız erişim yetkisi verilmez.
44. Uygulama geliştirme sürecinde görevlerin ayrılığı ilkesi doğrultusunda, yazılım geliştirme personelinin üretim ortamına erişimi engellenir.
45. Altyapı, sistemler ve kritik ağ araçları üzerinde yüksek yetkiye sahip kullanıcılara merkezi log yönetimi aracında yönetici yetkisi verilmez.

46. BT personeline ve tedarikçi firma personeline uygulama seviyesinde finansal işlem oluşturmayı sağlayacak erişim yetkileri verilmez.

47. Etkin bir görevler ayrılığı ortamının tesis edilebilmesi için A Ödeme verileri üzerinde etkileri olabilecek süreçleri yürütecek personele, kendilerine atanan görevler göz önünde bulundurularak, sadece bu görevleri yerine getirmelerine yetecek kadar yetkinin verilmesi temin edilir.

48. Görevlerin tam manasıyla ve uygun şekilde ayrıştırılmasının mümkün olmadığı durumlarda, bu durumdan kaynaklanabilecek hata ve suiistimalleri önlemeye yönelik risk azaltıcı veya telafi edici kontroller tesis edilir.

49. Bilgi sistemlerine ilişkin fonksiyonların gerçekleştirilmesinde görevler ayrılığı ilkesinin gereklerini sağlamak için tesis edilen kontrollerin aşılabilirliğini tespit etmek üzere testler yapılır.

6.5. Kullanıcı Kimlik ve Hesap Yönetimi Politikası

50. Bilgi sistemleri üzerinden gerçeklesen işlemler için kimlik doğrulama mekanizmaları kullanılır.

51. Hangi kimlik doğrulama tekniklerinin kullanılacağına, Risk Yönetim Müdürü tarafından yapılacak risk değerlendirmesi sonucuna göre karar verilir.

52. Risk değerlendirmesi, bilgi sistemleri üzerinden gerçekleştirilmesi planlanan işlemlerin türü (tipi, niteliği, varsa doğuracağı finansal ve finansal olmayan etkilerinin büyüklüğü gibi), işleme konu verinin hassaslık derecesi ve kimlik doğrulama tekniğinin kullanım kolaylığı da göz önünde bulundurularak gerçekleştirilir.

53. A Ödeme bünyesindeki yetkili ve standart kullanıcı hesaplarının yönetimi, bilgi sistemlerine ve uygulamalarına erişim ve kullanıcı hesapları şifrelerinin standartlara uygun şekilde oluşturulması, kullanılması, korunması, değiştirilmesi ve tanımlanan şifrelerle ilgili kullanıcıların bilgilendirilmesi süreci “Kullanıcı Kimlik ve Hesap Yönetimi Prosedürü” doğrultusunda gerçekleştirilir.

54. Yetkilendirme düzeyi ve erişim haklarının atanmasında ilgili unsurun görev ve sorumlulukları göz önünde bulundurularak, gerekli olacak en düşük yetkinin atanması ve en kısıtlı erişim hakkının verilmesi yaklaşımı esas alınır.

55. Kuruluş ağına; A Ödeme personeli tarafından ve dışından yapılacak erişimler “Kullanıcı

Hesabı Yönetimi Prosedürü" doğrultusunda detaylı bir şekilde düzenlenir. Tüm personelin bu talimat hükümleri uyarınca hareket etmesi esastır.

6.6. Fiziksel ve Çevresel Güvenlik

56. A Ödeme bilgi sistemlerinin zarar görmemesi ve diğer tüm kritik bilgi varlıklarının fiziksel ve çevresel tehditlerden korunması amacıyla sistem odasına ait fiziksel ve çevresel güvenlik önlemleri ile fiziksel ortam erişim yönetimi süreci "Fiziksel ve Çevresel Güvenlik Yönetimi Prosedürü" kapsamında tanımlanmıştır.
57. Tüm personelin bu prosedür hükümleri uyarınca hareket etmesi için gerekli kontroller ilgili bölümlerce uygulanır.

6.7. Bilgi Güvenliği Olay Yönetimi

58. Bilgi Güvenliği Olayları, A Ödeme'nin sahibi olduğu bilginin gizliliğini, bütünlüğünü ve/veya erişilebilirliğini kısmen etkileyen/ortadan kaldıran ve buna bağlı olarak, A Ödeme'nin operasyonel süreçlerinde aksamalara veya maddi kayıp ile itibar kaybı yaşamasına sebep olabilecek güvenlik ihlalleridir.
59. A Ödeme bilgi sistemlerinde ve ağlarında oluşabilecek güvenlik olaylarının en kısa sürede algılanması, sebeplerinin analiz edilmesi için yeterli verinin toplanması, olası sistem aksaklıklarının en kısa sürede çözümlenmesi, ihlallere ve saldırılara karşı alınacak aksiyonların belirlenmesi, ilgili yerlere raporlanması ve bilgi güvenliği ihlalleriyle ilgili risklerin minimize edilmesine ilişkin sorumluluklar ve aktiviteler "Güvenlik Olay Yönetimi Prosedürü" dahilinde tanımlanmaktadır.
60. Tüm personelin prosedür doğrultusunda belirlenen sürece uyumu ve güvenlik ihlallerini BT Müdürlüğü/Bilgi Güvenliği Sorumlusuna bildirmesi esastır.

6.8. E-posta Kullanım Esasları

61. A Ödeme bünyesinde e-posta güvenliği standardı, aşağıda belirtilen başlıklar altında kategorize edilmiştir:
62. E-posta sisteminin kullanımı sadece iş amaçlıdır ve bu amaç dışında kullanılamaz.
63. E-posta ile veri iletimi için "Veri Sınıflandırma Prosedürü" doğrultusunda belirlenen güvenlik hassasiyet derecelerinin ve veri iletimi kontrollerinin uygulanması esastır.
64. Kullanıcılar, A Ödeme dışındaki alıcılara e-posta gönderirken; A Ödeme güvenlik politikası ve ilgili standartlara uygun hareket etmekle yükümlüdür.

65. A Ödeme e-posta sistemleri, kısıtlı bir mesaj güvenliği sunar. Bunun sonucu olarak, kullanıcıların hassas içerikli mesajların gönderilmesine dair tüm tatbik edilebilir kurallara uygun hareket etmeleri şarttır.
66. İşle ilişkili olmayan alıcı listeleri oluşturulmaz ve bu listeler kayıt altına alınmaz.
67. Kullanıcılar, kendi hesaplarından gönderilen tüm e-postalardan sorumlu olup; kendi e-posta hesaplarının yetkisiz olarak kullanılmaması için gerekli tüm önlemleri almakla da yükümlüdürler.
68. Kullanıcılar, taciz olarak değerlendirilebilecek veya düşmanca bir çalışma ortamına sebebiyet verebilecek hiçbir e-posta mesajını oluşturmaz veya bu tabiattaki dışarıdan alınmış e-postalarını başkalarına iletmezler. Bu kapsama spam e-postaları ve belli bir cinsiyet, ırk, din veya cinsel tercih hakkında aşağılayıcı ifadeler içeren e-postaları da dahildir. E-posta hesapları kullanılarak zincir mesajlar iletilmez, oluşturulmaz veya sirküle edilmez.
69. İşletim sistemine giren veya bu sistemden gönderilen tüm mesajlar, içerik filtrelemesine tabi tutulmakta olup; bu çerçevede bloke edilebilir/karantina altına alınabilir veya derhal silinebilir.
70. Bloke edilmiş/karantina altına alınmış mesajlar; mesajın alıcısı söz konusu içeriğin iş ile ilgili olduğunu düşünüyorsa, söz konusu içeriğin gönderilmesi bekleniyorsa ve mesaj güvenilir bir kaynaktan gelmişse serbest bırakılır.
71. E-posta güvenliği için, A Ödeme bünyesinde kullanılan antivirüs yazılımları sürekli virüs taraması ve spam filtrelemesi gerçekleştirilir.
72. Virüs tanıma dosyası, otomatik olarak güncellenerek kontrolü sağlanır.

6.9. İnternet Kullanım Esasları

73. A Ödeme bünyesinde internetin kullanıcılar tarafından uygunsuz kullanımının önlenmesi ve A Ödeme'nin yasal yükümlülükleri, imajı ve çalışan performansı konularında istenmeyen sonuçlar ile karşılaşılmaması amacıyla internet kullanımının kontrolüne ilişkin esaslar aşağıdaki gibi düzenlenmiştir:
74. A Ödeme faaliyetleriyle ilgili iletişim ve bilgi edinme amaçlı internet kullanımı, kabul edilebilir internet kullanımı olarak değerlendirilir.
75. 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar

Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" gereğince; A Ödeme, sağladığı hizmetlere ilişkin, belirtilen internet erişim bilgilerini yasal süreler doğrultusunda kayıt altına alarak saklar ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlar.

76. A Ödeme itibarını ve faaliyetlerini güvence altına almak ve bilgi sistemleri ortamının veri bütünlüğünü ve sürekliliğini korumak için Kurum, yasalarca tanınan yetkiler çerçevesinde internet erişimini izleme, filtreleme ve bloke etme hattını saklı tutar.
77. A Ödeme güvenlik politikaları doğrultusunda web-filtreleme uygulaması tarafından içerik filtrelemesinin gerçekleştirilmesini sağlar ve yasaklı sitelere erişim engellenir (ahlak dışı, kumar, oyun, şiddet içeren vb.).
78. Kullanıcılar; başka sistemlerin güvenlik zaaflarını tespit etmek, yetki sahibi olmadıkları gizli bilgiler erişmek, diğer sistemleri tehlikeye düşürmek, herhangi bir veriyi yasadışı olarak tahrip etmek, yasadışı olarak program ve verilere sahip olmak veya transfer etmek veya kötü niyetli mesajlar göndermek için söz konusu sistemlere girmeye çalışamazlar.
79. BT Müdürünün onayı alınmadan kullanıcı bilgisayarlarına hiçbir yazılım programı indirilmez veya yüklenmez.
80. İnternet üzerinden Kurum ağına veri indirmek veri içeriği iç ve dış mevzuatlara uygun almak ile birlikte tüm verilerin uygun metot ve araçlar kullanılarak virüs taramasından geçirilmesi ile mümkündür.

6.10. Kullanıcı Bilgisayarları ve Taşınabilir Aygıtlar Kullanım Standartları

81. Kullanıcı bilgisayarlarının ve A Ödeme bilgi sistemlerinin zararlı yazılımların etkilerinden korunması ve güvenliğin sağlanması, lisanssız yazılımların kullanımının engellenmesi, bu yazılımların getirdiği güvenlik tehditlerinin tespit edilmesi ve gerekli önlemlerin alınabilmesi amacıyla aşağıdaki kontroller düzenlenmiştir:
82. A Ödeme çalışanlarına sunulan bilgisayarlar, sadece işe uygun amaçlarla kullanılır.
83. Kullanıcılar, kendilerine temin edilen cihazları Bilgi Güvenliği Politikasına uygun olarak kullanmak ve korumaktan sorumludur.
84. BT Bölümünün sağladığı alt yapıyı kullanarak ve prosedürleri izleyerek bilgisayarlardaki özel bilginin gizliliğinden, bütünlüğünden, bilgi kaybını önlemek amacıyla yedekleme ve kurtarma işlemleri ile bu bilgilerin yetkisiz kişilerin eline geçmesinin önlenmesinden

kullanıcılar sorumludur.

85. Kullanıcı bilgisayarlarında kullanılan işletim sistemi ve güvenlik yazılımlarına yönelik yamaların yönetimi, BT Bölümü tarafından gerçekleştirilir.

86. Kullanıcı bilgisayarlarına BT Bölümü tarafından belirlenen ve kullanıcı bilgisayarlarına yüklenmiş olan yazılımlar haricinde yazılım yükleyemez.

87. Taşınabilir aygıtlar yalnızca iş amaçlı olarak kullanılır. Söz konusu cihazların kullanımı, yetkilendirilmiş şahıslar tarafından gerçekleştirilse dahi; işle ilgili olmayan verilerin dağıtımında kullanılmaz.

88. Çalışanlar, taşınabilir aygıtlar dahilinde kullandığı/oluşturduğu bilgilerin önceden belirlenmiş ortak alanlarda yedeklemesinden ve arşivlenmesinden sorumludurlar.

89. Kullanımları altında taşınabilir bilgisayarlar, dizüstü bilgisayarlar, tablet bilgisayarlar, akıllı telefonlar ve diğer bu nevi taşınabilir bilgisayar veya depolama cihazları bulunan şahıslar; bu cihazlarda Kuruma ait kamuya açık olmayan bilgiler bulunduruyorsa; söz konusu bilgilerin usulüne uygun olarak korunmadığı durumlarda, bu cihazların güvenliğinin sağlanmasından sorumludur.

90. Şifrelenmediği müddetçe, gizli bilgilerin taşınabilir cihazlarda saklanması yasaktır.

91. Herhangi bir taşınabilir bilgisayar ekipmanının çalınması veya kaybedilmesi durumu, bir güvenlik ihlali olarak değerlendirilir ve “Güvenlik Olay Yönetimi Prosedürü’ne uygun olarak en kısa sürede raporlanır.

6.11. Temiz Ekran ve Temiz Masa Kullanım Standartları

92. A Ödeme bünyesinde kullanıcı bilgisayarlarının ve verilerin yetkisiz kullanımını engellemek amacıyla çalışanların günlük iş akışları sırasında dikkat etmesi gereken standartlar aşağıda belirtilmiştir:

93. Önemli bilgi içeren dokümanlar ve veri depolama cihazları (CD, DVD, flash disk vb.) kullanılmadığı zamanlarda veya mesai saatleri dışında güvenli alanlarda saklanır. Eğer bu doküman ve cihazların saklanabileceği güvenli kasa veya dolaplar mevcut değilse, bulundukları odanın kapısı kilitli tutulur. Eğer mümkünse önemli bilgiler sadece yetkisiz erişimlerden değil, bilgilerin yok olmasına neden olabilecek dış etkenlerden (yangın, sel vb.) de korunur.

94. Taşınabilir belleklerle transfer edilen tüm dosyalar ve veriler kullanıldıktan sonra silinir,

transfer haricinde bellekler üzerinde hiçbir veri tutulmaz. Aynı şekilde ortak alanlarda paylaşılan tüm dosyalar, transfer gerçekleştikten sonra hemen silinir.

95. Tüm taşınabilir cihazlar (dizüstü ve tablet bilgisayarlar, akıllı telefonlar, taşınabilir bellekler vb.) için şifreli ekran-koruyucular belirlenir ve hırsızlığa karşı özel kablolarla kilitlenir. Taşınabilir cihazlar kesinlikle ortalıkta bırakılmaz.
96. Bilgisayar ekranları, yetkisiz kişilerin göremeyeceği şekilde tutulur.
97. Kullanıcılar çalışma alanlarını terk ederken bilgisayar ekranlarını kilitler.
98. Şifreler yazılı olarak saklanmaz.
99. Mesai saatleri dışında, çalışma ortamları temiz ve düzenli bırakılır.
100. Eğer kullanılıyorsa flip-chart ve beyaz tahta gibi sunum ekipmanları üzerindeki yazılı bilgiler silinir.
101. Veri depolama cihazlarının saklandığı alanlar, her zaman kapalı ve kilitli tutulur.
102. Gizli dokümanlar çöp kovasına atılmamalıdır, iş bittiğinde dokümanlar parçalanarak atılmalıdır.
103. Çekmeceler kilitli tutulur ve anahtarlar göz önünden kaldırılarak saklanır.
104. Kritik bilgi içeren dokümanların çıktısı alındıktan sonra, ortalıkta bırakılmaz.

7. Politikanın İhlali

105. A Ödeme çalışanları veya üçüncü parti çalışanlar tarafından gerçekleştirilecek olan çalışmalarda, Bilgi Güvenliği Politikası ve politikanın işletilmesine yönelik oluşturulan prosedürlere uyum sağlanması zorunludur.
106. A Ödeme bünyesinde çalışan tüm personel ve alınan hizmet doğrultusunda gerek duyulursa üçüncü taraf firmaların politikaya uyum konusunda “Bilgi Güvenliği Uyum Taahhütnamesi” ile yazılı taahhütleri alınır.
107. Bu taahhütnameyi imzalayan tüm çalışanlar A Ödeme bünyesindeki politika, prosedür ve standartlarda belirtilen gizlilik ve güvenlik esaslarına uygun hareket etmeyi kabul etmiş sayılır.
108. A Ödeme, Bilgi Güvenliği Politikasının ihlali durumunda bu ihlalin ciddiyetine göre hareket etme hakkını saklı tutar; ancak Politikaya uymama veya kasıtlı politika ihlalleri durumunda, İnsan kaynakları politikasının, politika ihlali maddesi uygulanır.

8. Bilgi Güvenliği Politikasının Güncellenmesi

109. Bilgi Güvenliği Politikası yılda en az bir kez BT Sorumlu'su tarafından gözden geçirilerek, değişiklik/ihtiyaç halinde güncellenmesi sağlanır.

110. Güncellenen Bilgi Güvenliği Politikası İç Kontrol Sorumlusu görüşlerine sunulduktan sonra Yönetim Kurulu onayına sunulur. Politika Yönetim Kurulu tarafından onaylandığı takdirde, politika yayınlanarak tüm kullanıcılara haberleşme kanalları vasıtasıyla (Duyuru, Bilgi Güvenliği Farkındalık Eğitimi vb.) duyurulur.

Ekler

EK. 1 Bilgi Güvenliği Uyum Taahhütnamesi

EK. 2 Eğitim Katılım Formu