Akbank T.A.Ş.

Bilgi Teknolojileri Aracılığı ile Hizmet Sunan Tedarikçiler için Bilgi Güvenliği Standartları

Doküman Sahibi : Bilgi Riski Yönetimi Başkanlığı

Versiyon : 1.0

Versiyon Tarihi : 19.09.2024

İÇERİK

1 AMAÇ VE KAPSAM 3

2 TANIMLAR 3

3 STANDART 4

3.1 Bilgi Güvenliği Politikaları ve Yönetişimi 4
3.2 Veri Güvenliği 4
3.3 Kimlik Doğrulama ve Yetkilendirme 6
3.4 Uzak Bağlantı Yönetimi 9
3.5 Ağ ve İletişim Güvenliği 9
3.6 İz Kayıtları 10
3.7 Fiziksel Güvenlik 11
3.8 Uygulama ve Sistem Güvenliği 11
3.9 Güvenli Yazılım Geliştirme 12
3.10 Değişiklik Yönetimi 13
3.11 Zafiyet ve Tehdit Yönetimi 13
3.12 Müdahale ve İş Sürekliliği Planları 14
3.13 Alt Yükleniciler 14
3.14 Diğer 14

1 AMAÇ VE KAPSAM

Bu doküman bilgi teknolojileri aracılığı ile Banka'ya hizmet sağlayan ve/veya Banka bilgilerini saklayan, transfer eden, işleyen ve banka bilgilerine erişim sağlayarak hizmet sunan Tedarikçiler tarafından uyulması gerekli olan asgari bilgi güvenliği gereksinimlerinin belirlenmesi amacıyla oluşturulmuştur.

Bilgi güvenliği tedbir maddeleri içerisinde kapsam sınırlandırılmadığı sürece, belirtilen gereksinimler Tedarikçiler tarafından Banka'ya sunduğu hizmetlerle sınırlı olmak koşulu ile Bankaya sunulan hizmetlerde kullanılan bilgi sistemleri ve bu sistemlerin çalışmasını doğrudan ya da dolaylı olarak etkileyebilecek bilgi sistemleri için uygulanmalıdır.

Tedarikçilerin hizmet sunduğu faaliyet bölgesinde geçerli olan yasal ve düzenleyici gereklilikler ile sunduğu hizmet kapsamındaki özel sözleşme koşulları bu dokümanda belirtilenden daha kısıtlayıcı tedbirler uygulamasını gerektiriyor ise; Tedarikçi yasal, düzenleyici gereksinimler ve sözleşme koşullarına uygun hareket etmelidir.

Tedarikçi bu dokümanda tanımlanan ve sunduğu hizmet kapsamında uygulaması beklenen tedbirleri; teknik kısıtlamalar ve iş gereksinimlerinden dolayı bu dokümanda belirtildiği şekli ile karşılayamaması durumunda aynı amaç ve etkiye sahip olan telafi edici kontroller uygulamalıdır. Telafi edici kontrollerin uygunluğu Banka tarafından değerlendirilmeli ve Banka yazılı onayı alınmalıdır.

Tedarikçi bu dokümanda belirtilen gereksinimlerin yerine getirilmesine yönelik soru ve talepleri için Banka ile iletişime geçmelidir.

2 TANIMLAR

Banka **:**Akbank T.A.Ş ve İştirak şirketlerini ifade eder.

Bilgi Sistemleri : Bankaya sunulan hizmetlerde kullanılan bilginin toplanması, işlenmesi, saklanması, dağıtımı ve kullanımına yönelik insan kaynağı, operasyonel faaliyetler ve süreçler ile bunlarla etkileşim içinde bulunan bilgi teknolojilerini ifade eder.

Bilgi Teknolojileri **:**Herhangi bir biçimdeki verinin, girişinin yapılması, saklanması, işlenmesi, iletilmesi ve çıktılarının alınması için kullanılan donanım, yazılım, iletişim altyapısı ve ilgili diğer teknolojileri ifade eder. (Örneğin; masaüstü, dizüstü, mobil cihazlar, sunucular üzerindeki işletim sistemleri, veritabanları, uygulamalar, güvenlik duvarları, yönlendirici ve anahtarlama cihazları gibi)

Bilgi Varlığı **:**Bankaya hizmet sunulan faaliyetlerin yürütülmesinde kullanılan veriler ile bu verilerin taşındığı, saklandığı, iletildiği veya işlendiği sistem, yazılım, ağ cihazları, BT donanımları, iş süreçleri gibi Banka için değeri olan varlıkları ifade eder.

Tedarikçi **:**Bankaya bilgi sistemlerine ilişkin hizmet tedarik eden, banka bilgilerinin gizliliği, bütünlüğü ve erişilebilirliği ile bankacılık faaliyetlerinin güvenliğini ve sürekliliğini etkileme potansiyeli olan, Banka verilerine erişimi olan hizmet sağlayıcılardır.

3 STANDART

3.1 Bilgi Güvenliği Politikaları ve Yönetişimi

3.1.1. Endüstri pratikleri ile yasal ve düzenleyici gereksinimlerle uyumlu olarak, rol ve sorumlulukları içerecek şekilde bilgi güvenliği ile ilgili politika ve standartlar belirlenmeli ve dokümante edilmelidir. Politika ve standartlar onaylı, güncel ve çalışanların erişimine açık olmalıdır. Bilgi güvenliği politika ve standartları için düzenli olarak gözden geçirme çalışmaları yapılmalıdır.

3.1.2. Bilgi varlıklarının yetkisiz veya farkında olmadan değiştirilmesi ya da kötüye kullanımını önlemek amacıyla; erişim, değişiklik ve kullanıma ilişkin olarak görevler ayrılığı ilkesi mümkün olduğunca uygulanmalıdır. Alınan hizmet kapsamındaki kritik işlemlerde girişçi-onaycı mekanizması kurulmalıdır.

3.1.3. Bilgi güvenliği eğitimi ve farkındalığı için periyodik çalışmalar (eğitim, e-posta oltalama denemesi vb.) yapılmalıdır. Çalışmaların ölçümlenmesi ve raporlanması sağlanmalıdır.

3.1.4. Bilgi güvenliği eğitimi ve farkındalık çalışmaları tüm çalışanlar, yükleniciler ve geçici çalışanları da kapsayacak şekilde, asgari olarak aşağıdaki konuları içermelidir. Bilgi güvenliği farkındalık programı yıllık olarak gözden geçirilmelidir.

- Kabul edilebilir kullanım
- Bilgi varlıklarının sınıflandırılması ve işlenmesi
- Güvenli bilgi paylaşım yöntemleri
- Parola politikası
- Sosyal mühendislik
- İhlal olaylarının raporlanması
- Kötü amaçlı yazılımlar

3.1.5. Banka bilgilerine erişimi olan Tedarikçi çalışanlarının çalışma alanlarında yer alan fiziksel veya dijital bilgileri korumak için temiz masa temiz ekran prensipleri uygulanmalıdır.

3.1.6. Çalışanlardan Bilgi Güvenliği Politika ve Standartlarına uyum konusunda taahhüt alınmalı ve saklanmalıdır.

3.1.7. Tedarikçi bilgi güvenliği risk iştahını tanımlayan ve bilgi güvenliği risklerinin bu iştahla uyumlu olmasını sağlayan bir bilgi güvenliği risk yönetimi programı uygulamalıdır. Risk raporlamaları periyodik olarak üst yönetime yapılmalıdır. Tedarikçi bilgi güvenliği ile ilgili risk ve aksiyonların takibini yapmalıdır.

3.1.8. Uygulama, ürün ve hizmetlerin edinimi, geliştirilmesi ve kullanımı için bilgi güvenliği prosedürleri tanımlanmalı ve işletilmelidir.

3.1.9. Bilgi varlıkları (Yazılımlar, donanımlar vb.) için bir bilgi varlık envanteri oluşturulmalıdır. Envanterin tam, doğru ve güncel olması sağlanmalıdır. Her bir varlık için hesap verilebilirlik sağlanmalıdır.

3.2 Veri Güvenliği

3.2.1. Banka bilgileri Çok Gizli, Gizli, Kurum içi ve Kamuya açık Olmak üzere dört farklı gizlilik kategorisine ayrılır. Bilgilerin gizlilik kategorisine bağlı olarak Banka tarafından belirlenen

standartlara uygun hareket edilmelidir. Bilgilerin gizlilik kategorisine uygun ve yeterli seviyede koruma sağlanmalıdır.

3.2.2. Tedarikçi tarafından saklanan, iletilen, işlenen Banka bilgileri için yetkisiz erişimlere, değişikliklere ve silinmeye karşı güvenlik önlemleri alınmalıdır.

3.2.3. Tedarikçi tarafından yönetilmeyen cihazlarda (Kişisel bilgisayar, mobil telefon, mobil internet vb.) Banka Çok Gizli, Gizli ve Kurum İçi bilgileri işlenmemeli ve saklanmamalıdır. Bu bilgilerin Üçüncü bir taraf tarafından işlenmesi veya saklanmasını gerektiren durumlarda sözleşmelerin gizlilik hükümleri içermesi sağlanmalıdır. Bilgilerin üçüncü tarafa aktarımı öncesi Bankaya bilgi verilmeli; bilgilerin kullanımı ve silinmesi için özel politika, prosedür ve standartlar geliştirilmeli ve uygulanmalıdır.

3.2.4. Bankaya sunulan hizmet kapsamında elde edilen veriler iş ihtiyacı dışında ve Bankanın onayı olmaksızın 3. taraf kişi veya kurumlar ile paylaşılmamalıdır. Bankaya sunulan hizmet kapsamında bir alt yüklenici kullanıldığı durumda, alt yüklenici tarafından elde edilen verilerin amacı kapsamında kullandığının güvencesi sağlanmalıdır.

3.2.5. Bankaya sunulan hizmetlerde işlenen verilerin uçtan uca güvenliği sağlanmalıdır. Veri güvenliğine ilişkin standartlar oluşturulmalı ve standartlara uyum sağlanmalıdır.

3.2.6. Banka Gizli ve Çok Gizli bilgilerinin yazdırılması, kaydedilmesi veya kopyalanmasını kısıtlayıcı tedbirler uygulanmalıdır.

3.2.7. Bilgi paylaşımı için güvenli paylaşım yöntemleri ve protokolleri kullanılmalıdır. (Örneğin; SFTP, HTTPS ve SSH gibi)

3.2.8. İş ihtiyacı kalmayan bilgiler, bulunduğu ortam türüne uygun olarak; geri getirilemeyecek ve güvenli bir yöntemle imha edilmeli, imha işlemi kayıt altına alınmalı ve ihtiyaç halinde sunulabilmesi için imha kanıtları oluşturulmalıdır.

3.2.9. Banka bilgileri kimliksizleştirilmeden, maskelenmeden veya gizlenmeden geliştirme ve test ortamlarında kullanılmamalı ve saklanmamalıdır.

3.2.10. Gizli ve Çok Gizli bilgiler şifrelenmemiş olarak genel ağlar üzerinden iletilmemelidir. Bu bilgilerin genel ağlar üzerinden iletilmesi durumunda; güncel ve güvenli şifreleme algoritmaları ile şifreli olarak iletilmesi sağlanmalıdır.

3.2.11. Gizli ve Çok Gizli bilgilerin tedarikçi ağı dışında depolanması durumunda güncel ve güvenli bir şifreleme algoritması ile şifreli tutulması sağlanmalıdır.

3.2.12. Banka bilgilerinin güvenli olarak belirlenen cihazlarda güvenlik politikalarına uygun olarak saklanması sağlanmalıdır.

3.2.13. Banka bilgilerine erişen tüm çalışanları kapsayacak şekilde veri sızıntısı önleme (DLP) kontrolü tesis edilmelidir. Şifrelenmemiş e-postalar, şifreli e-posta ekleri, yazdırma, bulunduğu ağdan dış ağlara aktarma (Bir web sitesine yükleme vb.), taşınabilir disklere aktarım gibi durumlarda tespit edici ve önleyici tedbirlere sahip olmalıdır. Veri taşıma, iletme, kopyalama gibi girişim ve işlemler kaydedilmeli ve alarm üretmelidir.

3.2.14. Banka bilgilerine erişen tüm çalışanları kapsayan web erişim kontrolleri uygulanmalıdır. Bu kapsamda, veri sızıntısına yol açabilecek bulut veri ve nesne depolama ortamlarına, e-posta servislerine, anlık mesajlaşma uygulamalarına, sosyal medyaya erişimler kontrol altına alınmalı, kötü amaçlı kod ve saldırıya sebep verebilecek sitelere erişim engellenmelidir.

3.2.15. Web tarayıcılarının en son güvenlik güncellemeleri ile güncel tutulması sağlanmalıdır.

3.2.16. Anlık mesajlaşma ve işbirliği araçları Banka bilgileri için uygun şifreleme yöntemleri uygulanmadığı takdirde kullanılmamalıdır.

3.2.17. Banka bilgilerinin bulunduğu ağdan harici kişisel e-posta hesaplarına tedarikçi kullanıcılarının erişimleri kısıtlanmalıdır.

3.2.18. E-posta sistemleri üzerinde gelen dosya eklerinin taranması, zararlı dosyaların engellenmesi, antispam/antiphishing yazılımları, gizli verilerin şifrelenmesi gibi kontroller uygulanmalıdır. E-posta istemcileri en son güvenlik güncellemeleri ile güncel tutulmalıdır.

3.2.19. Tüm fiziksel ve dijital ortamlarda uygun güvenlik tedbirleri alınmalıdır. Banka bilgilerinin bulunduğu sistemlerde taşınabilir medya ve depolama cihazları için erişim izni verilmemelidir. İstisna tanımlanması durumunda uygun onay süreciyle yetki tanımlanmalı, veriler uygun şifreleme yöntemleri ile şifrelenmelidir. Taşınabilir medya ve depolama cihazlarına Banka bilgilerinin aktarılması durumunda, güvenli iletimini sağlamak için yeterli önlemler alınmalı ve teslimat durumu teyit edilmelidir.

3.2.20. Banka bilgileri yasa ve düzenlemeler gereği, sözleşmelerin sona ermesi akabinde veya ihtiyaç ortadan kalktığında tekrar kullanılmayacak ve kurtarılamayacak şekilde güvenli olarak imha edilmelidir. İmha sürecine ait kayıtlar saklanmalıdır.

3.2.21. Banka tarafından talep edilen banka bilgileri, mutabık kalınan periyotta güvenli iletim yöntemleri ile Bankaya iade edilmelidir.

3.2.22. Herhangi bir Gizli veya Çok Gizli bilgi Bankanın onayı olmaksızın internet üzerinden erişim sağlanan bir sistemde bulundurulmamalı ya da depolanmamalıdır.

3.2.23. Banka Gizli ve Çok Gizli bilgilerinin sesli olarak telaffuz edildiği tedarikçi lokasyonlarında, güvenlik kameraları ses kaydı almamalıdır.

3.2.24. Banka bilgilerine mobil cihazlardan erişim sağlanması durumunda, mobil cihazlar üzerinden veri çıkışına dair güvenlik kontrolleri (DLP, MDM araçları vb.) uygulanmalıdır.

3.2.25. Taşınabilir kullanıcı bilgisayarları için disk şifreleme yapılmalıdır.

3.2.26. Tedarikçi tarafından banka bilgilerinin saklanması ve iletimi sağlanıyorsa, Gizli ve Çok Gizli bilgiler için güncel ve güvenli şifreleme yöntemi kullanılmalıdır. Bankaya ait Gizli ve çok gizli bilgiler ayrı veri tabanlarında bulundurulmalıdır.

3.2.27. Gizli ve Çok Gizli bilgilerin iletimi için güncel durum itibarıyla güvenilirliğini yitirmemiş ve günün teknolojisine uygun algoritmalar ve güçlü şifre paketleri (cipher suites) kullanılmalıdır. Örneğin; TLS 1.2/1.3, şifre paketi: TLS 1.3 için TLS_AES_256_GCM_SHA384 (0x13, 0x02).

3.2.28. Gizli ve Çok Gizli bilgilerin Tedarikçi ortamında saklanan ve iletilen Gizli ve Çok Gizli Banka bilgileri için Gelişmiş Şifreleme Standardı AES kullanılmalı ve anahtar uzunluğu 256 bit veya üzeri olmalıdır.

3.2.29. Kriptografik mesaj özeti için SHA-2 ve SHA-3 ailesi kullanımı sağlanmalıdır.

3.3 Kimlik Doğrulama ve Yetkilendirme

3.3.1. Bilgi sistemlerine izinsiz erişimi önlemek için erişim kontrol mekanizmaları kurulmalıdır. Minimum yetki prensibine uyumlu olarak oluşturulan erişim kontrol mekanizmaları dokümante edilmeli ve denetlenebilir olmalıdır.

3.3.2. Yetkilendirmeler rol bazlı uygulanmalıdır ve rol ve yetki matrisleri hazırlanmalıdır.

3.3.3. Erişim yetkilendirmesi öncesinde uygun seviyede onay aşaması kurgulanmalı ve kayıt altına alınmalıdır.

3.3.4. Her bir kullanıcıya verilen ve geri alınan yetkilerin takibi ve izlenmesi için denetim mekanizması tesis edilmelidir.

3.3.5. İhtiyaç dışı kullanıcı yetkileri belirli aralıklarla gözden geçirilmelidir. Gözden geçirme süreci, doğrulama ve gereksiz erişimlerin kaldırılması işlemleri için prosedürler dokümante edilmeli ve onaylı olmalıdır.

3.3.6. İşten ayrılma ve görev değişikliği gibi nedenlerle erişim ihtiyacının ortadan kalkması durumunda, erişimin kaldırılması için prosedürler geliştirilmeli ve uygulanmalıdır.

3.3.7. Kullanıcılar için oturum veya işlem başlatılmadan önce kullanıcı kimliğini doğrulamak üzere güvenli kimlik doğrulama yöntemi uygulanmalıdır.

3.3.8. Kullanıcı kimlikleri tekil ve benzersiz olmalıdır.

3.3.9. Paylaşılan kimlik doğrulama altyapıları (Single sign on vb.) kimlik doğrulama gereksinimlerini karşılamalıdır.

3.3.10. Minimum aşağıdaki şartları karşılayan şifreler kullanılmalı ve bu prensipler dokümante edilmelidir.

- En az 8 karakter kullanılmalıdır.
- Tahmin edilmesi zor (1 Büyük, 1 Küçük harf, Rakam ve Özel karakter setinden 3 tanesini içermelidir) olmalıdır.
- Son kullanılan 5 parola kullanılamamalıdır.
- Max 90 günde şifre değiştirmeye zorlamalıdır.
- İlk giriş/sıfırlamada şifre değiştirmeye zorlamalıdır.
- Son şifre değişikliğinden en az 1 gün sonra şifre yeniden değiştirilebilmelidir.
- 5 yanlış şifre deneme sonrasında kullanıcı hesabı bloke olmalıdır.
- 180 gün kullanılmayan kullanıcı hesapları kontrollü olarak kapatılmalıdır.

3.3.11. Kullanıcı hesapları ortak olarak kullanılmamalı, kullanım zorunlu ise kullanıcıyı ayırt edecek mekanizmalar oluşturulmalıdır.

3.3.12. Uygulama/sistem şifrelerinin geri dönülemez bir şekilde şifreli olarak saklanması sağlanmalıdır.

3.3.13. Tedarikçi ağı dışından erişimler, minimum ihtiyaç prensibince sınırlandırılmalı, erişimde VPN, ZTNA gibi modern yöntemler ve çok faktörlü kimlik doğrulama kullanılmalıdır.

3.3.14. Tedarikçi bilgi sistemlerine uzaktan bağlantı oluşturulması durumunda tüm iletişimin şifreli yapıldığından emin olunmalıdır.

3.3.15. Kullanıcı yönetimi (tanımlama, silme, yetkilendirme vb.) işlemleri için IP, kullanıcı kodu, tarih, saat, yapılan işlem detayı ile denetim iz kaydı tutulmalıdır.

3.3.16. Son kullanıcılara sistemlerde (sunucu, bilgisayar vb.) yönetici (local veya domain admin) yetkileri verilmemelidir.

3.3.17. Banka bilgilerinin bulunduğu ortamlara (ses, kart, müşteri vb verilerin saklandığı sunucu/klasör/disk vb.) erişim yetkileri kısıtlanmalıdır.

3.3.18. Domain Admin (Etki alanı yöneticisi) kullanıcısının yalnızca Active Directory sunucusunda kullanılması sağlanmalıdır.

3.3.19. Yerel yönetici grubu üyelerine ekleme veya çıkarma olduğunda alarm üretilmeli, grup üyeleri periyodik olarak kontrol edilmelidir.

3.3.20. Kullanıcı bilgisayarlarında yerel yönetici şifrelerinin farklılaştırılmasını sağlayacak çözümler kullanılmalıdır.

3.3.21. Bilgi sistemlerine erişimde merkezi kimlik doğrulama sistemleri kullanılmalıdır. (Active Directory, LDAP vb.)

3.3.22. Hiçbir işlem yapılmayan hareketsiz oturumlar için oturumun belirli bir süre sonra sonlandırması veya kilitlemesi için gerekli teknik tedbirler oluşturulmalıdır.

3.3.23. Kullanıcı "login" işlemlerinde kimlik doğrulama adımında kullanıcının hatalı bir giriş yapması nedeniyle gösterilecek hata mesajında hatanın kaynağına dair bilgi verilmemeli ve genel hata mesajları gösterilmelidir.

3.3.24. Kullanıcı statik parolaları ekranda açık metin olarak gösterilmemelidir.

3.3.25. Bilgi sistemleri üzerinde uygun yetkilendirmeler veya tespit edici mekanizmalar olmaksızın görevler ayrılığı ilkesine aykırılık oluşturacak durumlara karşı doğrulama ve yetkilendirme süreçleri oluşturulmalıdır.

3.3.26. Tüm erişimler için denetim izi kayıtları oluşturulmalıdır.

3.3.27. Sistem yöneticileri, güvenlik duvarı yöneticileri, web siteleri yöneticileri gibi ayrıcalıklı veya yönetici yetkileri ile sistemlere erişimlerinde veya sistemlere erişmek için kullanılacak şifrelere erişimlerinde çok faktörlü kimlik doğrulama yöntemleri uygulanmalı, erişimler kaydedilmeli ve izlenmelidir.

3.3.28. Kullanıcı hesaplarında (varsayılan) default kullanıcı adı/şifre kullanılmamalıdır. Eğer kullanılması zorunda ise şifresi değiştirilmelidir. Tüm varsayılan kullanıcı hesapları için şifreler düzenli olarak değiştirilmeye zorlanmalıdır.

3.3.29. Ayrıcalıklı ve yönetici rolündeki tüm kullanıcı hesaplarının envanteri tutulmalıdır. Ayrıcalıklı ve yönetici rolündeki kullanıcı hesaplarının tanımlanması, kaldırılması ve kullanımına yönelik prosedürler geliştirilmeli ve uygulanmalıdır.

3.3.30. Erişim izinleri kayıt altında alınmalıdır. Ayrıcalıklı ve yönetici erişimleri önceden onaylanmış onay prosedürlerine göre onay verildikten sonra sağlanabilmelidir. Erişim gerekçesi onay sürecinin parçası olarak kayıt altına alınmalıdır.

3.3.31. Ayrıcalıklı ve yönetici kullanıcılarla açılan oturumlarda internete erişim ve haberleşme (e-posta, web sitelerine erişim gibi) işlevlerinin kısıtlanması sağlanmalıdır. Ayrıcalıklı kullanıcı ile sadece ayrıcalık kullanımı gerektiren fonksiyon yerine getirilmelidir.

3.3.32. Kullanıcı şifreleri konfigürasyon dosyaları, yazılım kaynak kodları ve veri tabanları dahil olmak üzere herhangi bir yerde veya dosyada açık metin olarak saklanmamalıdır.

3.3.33. Sistemlere/uygulamalara tanımlı ortak kullanıcı hesapları için aşağıdaki prensipler uygulanmalıdır:

- Şifreleri bilinmemelidir.
- Şifreleri konfigürasyon dosyaları vb. ortamlarda açık olarak saklanmamalıdır.

3.3.34. Active Directory de dâhil üretim ortamındaki tüm sunuculara erişimler ayrı ve izole bir bilgisayardan yapılmalıdır. İzole bilgisayar için önerilen kontroller aşağıdaki gibidir, gerekli kontrollerin uygulanması konusunda makul çaba sağlanmalıdır.

- Normal kullanıcı segmenti dışında ayrı ve izole bir segmentte yer almalıdır.
- İnternete erişimi olmamalıdır.
- E-posta erişimi olmamalıdır.
- Sunuculara erişimler için ayrı bir kullanıcı tanımlı olmalıdır.

3.3.35. Tedarikçi çalışanlarının, Banka sistemlerine bağlanması durumunda Banka'nın uygun gördüğü erişim kuralları ve rolleri ile uyumlu hareket edilmelidir.

3.4 Uzak Bağlantı Yönetimi

3.4.1. Banka verilerinin depolandığı, işlendiği ve iletildiği tüm ağlara uzaktan erişim yetkisiz erişimlere karşı korunmalıdır.

3.4.2. Uzaktan bağlantı için onaylı uzaktan erişim uygulamaları kullanılmalı ve yalnızca çok faktörlü kimlik doğrulama ile erişim sağlanmalıdır. Uzaktan erişimler için iz kayıtları saklanmalı ve izlenmelidir.

3.4.3. Tedarikçiye ait cihazların tedarikçi ağı dışında bir ağ bağlantısı gerçekleştirdiği durumda kişisel bir güvenlik duvarı etkin olmalıdır.

3.4.4. Tedarikçi tarafından yönetilen cihazlar uzak ağ bağlantısı için güncel yazılım ve anti virüs güncellemelerini almış olmalıdır.

3.4.5. Tedarikçiye ait olmayan cihazlar ile Banka bilgilerinin yer aldığı tedarikçi sistemlerine uzaktan erişim yapılmamalıdır.

3.4.6. Güvenli uzaktan erişim çözümleri devre dışı bırakılamamalıdır.

3.4.7. Üretim ortamında yer alan sistemlere yapılacak uzak bağlantıların şifreli olması sağlanmalıdır. (Örneğin; SSH, SSL özellikli web yönetim arayüzleri ve VPN çözümleri gibi)

3.4.8. İhtiyaç halinde tedarikçi ağına uzak erişim için VPN kullanıldığı durumlarda, split tunnel kullanılmamalıdır. (Online collaboration uygulamaları için diğer sistemleri riske atmayacak biçimde izin verilebilir.) VPN ile bağlantı yapılan cihazın VPN'e bağlı kaldığı süre içinde doğrudan internete erişimi olmamalıdır.

3.4.9. Uzaktan çalışma ortamında video/fotoğraf/ses kayıt cihazları bulundurulmamalı, yetkisiz kişiler tarafından fiziksel veya dijital ortamda bulunan verilerin ve uygulamaların görülmesi engellenmelidir.

3.5 Ağ ve İletişim Güvenliği

3.5.1. Tedarikçi ağ güvenliği için güvenlik duvarı, saldırı tespit ve önleme sistemi gibi güvenlik çözümleri ile uygun seviyede korunmalıdır. Tedarikçi ağına dışarıdan yapılan tüm bağlantılar güvenlik duvarı ile korunmalıdır.

3.5.2. Alınan hizmeti yansıtan, güncel bir ağ topolojisi bulunmalıdır.(IP bilgisi detaylarıyla)

3.5.3. Tedarikçi ağında yer alan bankaya sunulan hizmetlerde kullanılan tüm sistemler ayrı bir VLAN'a alınarak gerekli segmentasyon/izolasyon yapılmalıdır.

3.5.4. İnternet üzerinden erişilebilen tüm sistemler DMZ'de konumlandırılmalıdır.

3.5.5. Güvenlik sistemlerinde yapılacak değişikliklerde talep/ onay/ kayıt altına alma/ görevler ayrılığı/ test/ loglama prensipleri uygulanmalıdır.

3.5.6. Güvenlik duvarları için varsayılan bir "tümünü reddet" kuralı ve en az ayrıcalık prensibi uygulanmalıdır. Güvenlik duvarı kuralları periyodik olarak gözden geçirilmeli, gerekli sıkılaştırmalar yapılmalı, sonuçlar dokümante edilmelidir.

3.5.7. Bünyesinde Banka Gizli ve Çok Gizli bilgilerini içeren sunucuların (veritabanı sunucusu vb.) direkt olarak internete erişimi ve internet üzerinden bu sunuculara direkt erişim engellenmelidir.

3.5.8. Tedarikçi, güvenlik duvarı, ağ saldırı tespit ve engelleme sistemleri gibi uygulamaları içeren ancak bu uygulamalarla sınırlı olmayan katmanlı güvenlik savunması oluşturmalıdır. Güvenlik

sistemleri endüstri standartlarına uygun olarak yapılandırmalıdır. Güvenlik sistemlerinin sürekli izlenmesi için süreç oluşturmalı ve uygulanmalıdır.

3.5.9. Bankanın talebi halinde, herhangi bir zafiyet ve tehdit bildirimi sebebiyle bankaya hizmet veren spesifik sistem bileşenlerine erişim derhal kısıtlanmalıdır. Güvenlik olaylarının etkisini azaltmak için ağlar arasında erişim filtrelenebilmelidir.

3.5.10. Kablosuz ağlarda endüstri standartlarına uygun algoritmalarla haberleşme şifreli sağlanmalıdır. Kablosuz ağlara yetkisiz erişimi engellemek için makul seviyede tedbirler uygulanmalıdır.

3.5.11. Tedarikçi sistemlerinde barındırılan Banka servislerine uygun seviyede koruma sağlamak için anti-DDOS uygulama ve/veya hizmetleri kullanılmalıdır.

3.5.12. Veri transferi sırasında veri gizliliğini sağlamada kullanılacak şifreleme teknikleri için güncel durum itibarıyla güvenilirliğini yitirmemiş ve günün teknolojisine uygun algoritmalar kullanılmalıdır. (Örneğin TLS son versiyonu veya bir önceki güvenlik yamaları yapılmış versiyonu)

3.6 İz Kayıtları

3.6.1. Bilgi sistemlerinde gerçekleştirilen işlemlere dair denetim izleri yeterli detayda alınmalı, alarmlar oluşturulmalı ve düzenli olarak gözden geçirilmelidir.

3.6.2. Denetim izleri asgari olarak aşağıdakileri kapsamalıdır.

- Sistem güvenliğini ihlal edecek girişimler
- Bir güvenlik olayı ile ilişkili sistem alarmları
- Finansal işlemler veya Banka bilgilerini de içeren önemli olaylar
- Güvenlik yapılandırmaları ayarlarında değişiklikler
- Kullanıcı oluşturma, yetkilendirme, silme, şifre işlemleri
- Ayrıcalıklı ve yönetici kullanıcı hesapları ve işlemleri

3.6.3. Denetim izi kayıtları aşağıdaki bilgileri içermelidir.

- Kaydı oluşturan sistem
- Kaydın oluşturulduğu tarih, saat ve zaman dilimi bilgisi
- Kaydı oluşturan işlem ya da olayla birlikte, gerçekleştirilen değişikliğin ne olduğunu gösteren bilgi
- Kaydın ilişkili olduğu tekil kullanıcıyı veya sistemi gösteren bilgi

3.6.4. Denetim izi kayıtları asgari beş yıl boyunca tedarikçi nezdinde saklanmalıdır.

3.6.5. Denetim izlerinin yetkisiz erişim, değiştirilme ve silmeye karşı korunması için önlemler uygulanmalıdır.

3.6.6. Ortamda güvenilir ve doğru bir merkezi zaman sunucusu olmalıdır. Tüm sistemlerin saatleri merkezi bir zaman sunucusu tarafından ayarlanmalı ve değiştirilememelidir.

3.6.7. Güvenlik olayları ile ilişkili alarmlar belirlenmeli, kaydedilmeli ve izlenmelidir.

3.6.8. Kaydedilen olay kayıtlarının bir alarmı tetiklemesi durumunda, olay gözden geçirilmeli, ve bilgi güvenliği olayına sebep olduğu durumlarda inceleme yapılmalıdır.

3.6.9. Denetim izlerinin korelasyon analizi ve incelenmesi için SIEM veya merkezi analitik araçlarda toplanması sağlanmalıdır. Merkezi denetim izlerinin toplandığı uygulamaların yapılandırmaları periyodik olarak gözden geçirilmelidir.

3.7 Fiziksel Güvenlik

3.7.1. Tedarikçiye ait bilgi sistemleri cihazları, banka bilgilerinin bulunduğu tüm fiziksel ve elektronik ortamlar (Arşivler ve yedekleme alanları dahil) güvenli alanlarda bulundurulmalı ve iş ihtiyacına uygun olarak izinsiz erişimi sınırlandıran fiziksel güvenlik önlemleri alınmalıdır.

3.7.2. Bilgi sistemlerine fiziksel erişim için yasal ve düzenleyici gereksinimlere ve endüstri standartlarına uygun prosedürler tanımlanmalıdır.

3.7.3. Tesislere, sistem odalarına ve sistemlerin bulunduğu güvenli alanlara giriş/çıkışa dair kayıtlar (yeterli açıda görüş sağlayan kamera, kartlı giriş, ziyaretçiler için ziyaretçi defteri vb.), yeterli detayda (başarılı-başarısız erişim, erişen kişi, tarih, saat vb.) ve yeterli süre (en az 1 yıl) boyunca tutulmalıdır.

3.7.4. Tesislere ve sistemlerin yer aldığı güvenli alanlara giriş yetkileri minimum iş ihtiyacına göre sınırlandırılmalı, erişim yetkileri ve yetkisiz erişim denemeleri düzenli olarak gözden geçirilmelidir.

3.7.5. Çevresel tehditlere yönelik yeterli fiziksel güvenlik önlemleri (duman, yangın, su, sıcaklık, nem dedektörleri, alarm sistemleri, söndürme sistemleri, UPS, Jeneratör, kablolama düzeni vs.) alınmalı, bu sistemlerin düzenli bakımları ve testleri yapılmalı ve bu sistemlerden gelen kritik alarmlar izlenmelidir.

3.7.6. Bilgi sistemleri cihazlarına fiziksel olarak sadece yetki kişiler erişim sağlamalıdır.

3.7.7. Tüm ziyaretçiler için tesislere ve güvenli alanlara giriş ve çıkışlarda doğrulanabilir bir kimlik bilgisi sağlama zorunluluğunu içeren fiziksel güvenlik prosedürleri uygulamalıdır.

3.8 Uygulama ve Sistem Güvenliği

3.8.1. Bilgi sistemleri ve bilgi sistemleri kimlik doğrulama mekanizmaları iyi uygulama pratiklerine göre konfigüre edilmelidir.

3.8.2. Üretim sistemlerine yapılan kullanıcı erişimleri şifreli bağlantılar (örn. SSH, SCP, SSL özellikli web yönetim arayüzleri ve VPN çözümleri) üzerinden yapılmalıdır.

3.8.3. Bilgi sistemlerinde virüs ve kötü amaçlı yazılımlara/kodlara karşı tespit ve koruma uygulamaları konumlandırılmalıdır, bu uygulamaların güncelliği ve etkin olarak çalışırlığı sağlanmalıdır.

3.8.4. E-postalar, sunucular ve ilgili tüm uygulamalarda gerekli güvenlik taramalarını (antispam, antivirüs vb.) yapmalıdır. Kötü amaçlı hareketlerin tespit edilmesi durumunda derhal Banka'ya bildirilmesi sağlanmalıdır.

3.8.5. Tüm bilgisayarlar için BIOS ön yükleme sıralaması (boot order) CD/DVD, USB ve ağ adaptörü öncelikli olmayacak şekilde yapılandırılmalıdır, BIOS'a giriş parola ile korunmalıdır.

3.8.6. Bilgi sistemleri için güvenlik konfigürasyon standartları belirlenmeli ve bu standartlara uygun olarak sıkılaştırmalar yapılmalıdır. Güvenlik konfigürasyonunda yapılacak tüm değişiklikler yönetim tarafından onaylı bir değişiklik yönetimi sürecinden geçtikten sonra uygulanmalıdır.

3.8.7. Bilgi sistemleri için ihtiyaç duyulmayan uygulamalar ve işletim sistemi servisleri kaldırılmalıdır.

3.8.8. Makul seviyede bir güvenlik sağlayacak telafi edici kontroller oluşturulmadığı sürece, üretici desteği kesilmiş (end of support) bilgi sistemleri tedarikçi tarafından kullanılmamalıdır.

3.8.9. Bilgi sistemlerine yönelik güvenlik güncellemeleri takip edilmeli, test edilmeli, kontrollü ve gecikmeye mahal vermeden, hizmetlerde kesinti yaratmayacağından emin olunarak uygulanmalıdır.

3.8.10. Tedarikçi bilgi sistemleri ve uygulamaları için, BDDK Bilgi Sistemlerine İlişkin Sızma Testleri Genelgesine uygun olarak aşağıda belirtilen kapsamda yılda asgari 1 defa sızma testi gerçekleştirilmeli ve sonuçları Banka ile paylaşılmalıdır.

- İletişim altyapısı ve aktif cihazlar
- DNS Servis ve sunucuları
- Etki alanı(domain) ve son kullanıcı bilgisayarları
- E-posta servisleri
- Veritabanı sistem ve sunucuları
- Web uygulamaları ve web servisler
- Mobil uygulamalar
- Kablosuz ağ sistemleri ve cihazları
- DDoS testleri
- Sosyal Mühendislik Testleri

3.9 Güvenli Yazılım Geliştirme

Bu maddeler yalnızca Banka için yazılım geliştiren veya bankaya verdiği hizmette kullandığı yazılımları kendisi geliştiren tedarikçiler tarafından uygulanmalıdır.

3.9.1. Yazılım geliştirme yaşam döngüsü süreci dokümante edilmiş, güncel ve onaylı olmalıdır.

3.9.2. Güvenli yazışım geliştirme süreci oluşturulmalı, bu bağlamda yazılım döngüsü içerisinde asgari olarak aşağıdaki kontroller tesis edilmelidir.

- Planlama aşamasında güvenlik gereksinimleri belirlenmelidir.
- Geliştirme aşamasında yazılımın belirlenen güvenlik gereksinimlerinin dikkate alınarak geliştirilmelidir ve geliştirme yapılırken güvenli kod geliştirme pratikleri uygulanmalıdır.
- Derleme aşamasında yetkisiz ve kontrolsüz değişiklik yapılmasının önüne geçecek güvenli derleme prosedürleri uygulanmalıdır.
- Test aşamasında belirlenen güvenlik gereksinimlerinin uygulanmasına ve yazılımın güvenlik zafiyeti içermediğine yönelik testler yapılmalıdır.
- Sürüm ve dağıtım aşamasında geliştirilen yazılımın güvenli bir şekilde dağıtılmasına yönelik kontroller ile versiyonlama ve sürüm kontrollerine dayanan bütünlük kontrolleri uygulanmalıdır.
- Yazılım geliştirme yaşam döngüsünde DevSecOps pratikleri uygulanmalıdır.

3.9.3. Güvenli yazılım geliştirme eğitimleri düzenli olarak yazılım geliştiren çalışanlara verilmeli ve güvenli kodlama imkanı sağlayan uygulamalar kullanılmalıdır.

3.9.4. Banka adına geliştirilen/geliştirilecek olan internete açık uygulamalar için, OWASP uygulama güvenliği (Güncel OWASP Top 10 Web, Mobil, API) standartlarına uygun olarak geliştirilmelidir.

3.9.5. Kullanılan açık kaynak kütüphaneleri (open source library) kritik zafiyetler içermemelidir. Zafiyetler ele alınırken CVSS skoru dikkate alınarak önceliklendirme yapılmalıdır.

3.9.6. İnternete açık bir uygulama geliştirilmesi durumunda çok faktörlü kimlik doğrulama uygulanmalıdır.

3.9.7. Bankaya sunulan ürün veya hizmetler içinde sunulan fonksiyonların dışında başka bir özel fonksiyon veya açıklık, arka kapı gibi özellikler olmadığı taahhüt edilmelidir.

3.9.8. Tedarikçi geliştirdiği, barındırdığı veya tedarik ettiği yazılımlar için kötü amaçlı kod/ yazılımlara karşı kod gözden geçirme faaliyeti (SAST) ve yetkisiz erişim, veri ifşası, dolandırıcılık, veri bütünlüğünün bozulması, erişim ve performans problemleri gibi bilgi güvenliği zafiyetlerine ilişkin banka tarafından kabul edilebilir seviyede uygun güvenlik tarama testleri, sızma testleri, dinamik uygulama güvenlik testleri (DAST) gerçekleştirmelidir.

3.10 Değişiklik Yönetimi

3.10.1. Değişiklik yönetimi ile ilgili politika/süreç/rol/sorumluluk/sorumlu kişiler belirlenmiş, dokümante, onaylı, güncel ve çalışanların erişimine açık olmalıdır.

3.10.2. Değişiklik taleplerinde onay süreci, değişikliğin kayıt altına alınması, uygun testlerin yapılması sağlanmalıdır. Canlı ortama geçiş sırasında iz kayıtlarının oluşturulması sağlanmalı ve görevler ayrılığı ilkesine uygun hareket edilmelidir.

3.10.3. Geliştirme, test ve canlı ortamlar birbirinden ayrıştırılmış olmalıdır.

3.10.4. Canlı ortama aktarım yapılmadan önce versiyonlama yapılması, yedek alınması geri dönüş planı hazırlanması ve test edilmesi sağlanmalıdır. Test onayı alınan kodun canlıya alındığından emin olunmalıdır.

3.10.5. Güvenlik duvarları, IDS/IPS gibi güvenlik sistemlerinde yapılan değişiklikler tedarikçinin değişiklik yönetimi sürecine uygun olarak ele alınmalıdır.

3.10.6. Üretim ortamlarına yapılan tüm erişimler ve değişiklikler kaydedilmeli ve belirli periyotlar ile gözden geçirilerek örneklem metoduyla incelenmelidir.

3.10.7. Güvenlik risklerini asgariye indirecek bir yama yönetim programı oluşturulmalıdır. İlgili program sistemlere erişimde kullanılan her tür donanım ve yazılımı kapsamalıdır.

3.10.8. Bilgi sistemlerine yönelik yamalar ve dağıtımlar tedarikçi tarafından test edildikten ve onaylandıktan sonra diğer sistemlere yapılandırılmalıdır.

3.11 Zafiyet ve Tehdit Yönetimi

3.11.1. Güvenilir tehdit istihbarat kaynaklarını izlemek ve uygulamak için makul çaba göstermeli ve gerekli güvenlik kontrollerini uygulamalıdır.

3.11.2. Güvenlik açığı tarama araçları ile ağ ve sistemler taranmalı, kod analizi testleri ve sızma testleri gerçekleştirilmelidir.

- Güvenlik açıkları önem derecelerine sınıflandırılmalıdır.
- Her üretime geçiş öncesi değişiklik kapsamında ve yıllık olarak sistemin geneli için güvenlik taramaları yapılmalı ve tespit edilen açıkların düzeltilmesi sağlanmalıdır.

- Kritik güvenlik açıklarının öncelikli ele alınması sağlanmalıdır.

3.11.3. Tedarikçi bilgi sistemlerindeki tüm faaliyetler için oturum kayıtları, erişim denemeleri, güvenlik yapılandırma ayarları gibi sistem faaliyetleri için iz kayıtları tutulmalıdır. İz kayıtları yetkisiz erişim ve değişiklik/silmeye karşı korunmalıdır.

3.11.4. Bankayı etkileyen bir ürün veya hizmete yönelik kritik güvenlik zafiyeti tespit edildiğinde, tedarikçi Bankayı ivedilikle ve yazılı olarak bilgilendirmeli ve Banka tarafından talep edilen süre içerisinde güvenlik açığının giderilmesi sağlanmalıdır.

3.11.5. Tedarikçi, bilgi sistemlerinde herhangi bir güvenlik ihlali yaşaması durumunda ivedi olarak Banka'da belirlenmiş irtibat kişilerine ve/veya iletişim adreslerine bilgi vermelidir.

3.11.6. Tedarikçi bilgi güvenliği olaylarına etkili müdahale gerçekleştirmek üzere bir bilgi güvenliği olay yönetimi süreci oluşturmalı, dokümante etmeli ve uygulamalıdır. Bilgi güvenliği olay müdahale prosedürleri, Banka ve paydaşları açısından olayın etkilerinin (finansal sonuçları, itibar etkisi ve regülasyon etkileri) değerlendirmesini içermelidir.

3.11.7. Bankaya sunulan hizmetleri ve Banka bilgilerinin gizlilik, bütünlük ve erişilebilirliğini etkileyen tüm bilgi güvenliği olayları meydana geliş şeklinden bağımsız olarak ivedilikle Banka'ya bildirilmelidir.

3.12 Müdahale ve İş Sürekliliği Planları

3.12.1. Tedarikçinin bankaya verdiği hizmeti etkileyebilecek olaylara dair müdahale ve iş sürekliliği planları ve diğer siber güvenlik planları oluşturulmuş, işletilmiş ve iyileştirilebilir olmalıdır.

3.13 Alt Yükleniciler

3.13.1. Banka bilgi varlıklarına erişimi olan alt yükleniciler ile yapılacak anlaşmalarda bilgi güvenliği gereksinimlerine yer verildiğinden emin olunmalıdır.

3.13.2. Bankaya sunulacak hizmetlerde alt yüklenici ile çalışılması öncesinde Bankaya bilgi verilmeli ve onayı alınmalıdır.

3.13.3. Tedarikçi, Bankaya sunulacak hizmetlerde rol alan alt yüklenici ile sözleşme öncesi ve sonrasında makul güvence sağlayan bir bilgi güvenliği değerlendirme anketi veya eşdeğer bir kontrol ortamı ile alt yüklenici için bilgi güvenliği risk değerlendirmesi yürütmelidir.

3.13.4. Tedarikçinin birlikte çalıştığı alt yüklenicilerin banka verisine erişimi olması durumunda bu standarttaki maddelerin alt yüklenici tarafından da uygulandığından emin olunmalıdır.

3.14 Diğer

3.14.1. Kanun ve yasal düzenlemeler bu dokümanda yer alan hususlardan daha sıkı bir güvenlik kontrolü gerektiriyor ise, Tedarikçi ilgili kanun, mevzuat ve düzenlemelere uygun hareket etmelidir.

3.14.2. Tedarikçinin Banka'ya sunduğu hizmetin kapsamında Ödeme Kartları ile ilgili bir hizmet(ler) bulunması durumunda, Ödeme Kartları Endüstrisi Standartları'nın (PCI-DSS) ilgili hükümlerine uyumlu olmalıdır.

3.14.3. Banka ile Dış veya Destek hizmeti sözleşmesi kapsamında olan tedarikçiler, yasal gerekliliklere, politikaların, prosedürlerin ve kontrollerin uyumluluğu için Banka'nın üçüncü taraf değerlendirme sürecine tabidir.