

TEDARİKÇİLER İÇİN CİTİ GEREKLİLİKLERİ

SAHİPLERİ:
Citi Satın Alma ve Risk Başkanı

DÜZENLENME TARİHİ:
Ocak 2015

REVİZYON TARİHİ:
Eylül 2026

SÜRÜM:
9

İÇİNDEKİLER

1	GENEL BAKIŞ	3
2	EŞİT İSTİHDAM FIRSATI	5
3	RÜŞVET VE YOLSUZLUKLA MÜCADELE (AB&C)	6
4	HEDİYELER VE AĞIRLAMA	6
5	TEDARİKÇİ KATILIMI VE TEDARİKÇİ İLKELERİ	7
6	MODERN KÖLELİĞİN YASAKLANMASI	7
7	TEDARİKÇİ PERSONELİ	9
8	DOLANDIRICILIK YÖNETİMİ	10
9	MEDYA ETKİLEŞİMİ VE KAMUOYUNUN ÖNÜNE ÇIKMA	12
10	YAZILI ELEKTRONİK İLETİŞİMLER	13
11	SİYASİ FAALİYETLER VE KATKILAR	13
12	KARA PARA AKLAMA İLE MÜCADELE (“AML”)	14
13	KAYIT YÖNETİMİ	16
14	KURUMSAL DİRENÇ/İŞ SÜREKLİLİĞİ	17
15	GLOBAL ARKA PLAN TARAMASI STANDARTLARI	23
16	GİDERLER	25
17	BİLGİ GÜVENLİĞİ (IS)	26
18	GÜVENLİ İŞ YERİ KURALLARI	61
19	YAPAY ZEKÂ/MAKİNE ÖĞRENİMİ (ÜRETKEN YAPAY ZEKÂ/AJAN YAPAY ZEKÂ DÂHİL)	62
20	MÜŞTERİ ŞİKÂyetLERİ	63
21	KİŞİSEL TİCARET VE YATIRIM POLİTİKASI	63
22	FATURALANDIRMA VE FATURALAMA STANDARTLARI	64
23	ZORUNLU UZAKLAŞTIRMA POLİTİKASI	64
	EK - TANIMLAR	66

1 GENEL BAKIŞ

1.1. Genel Gereklilikler

Tedarikçilere Yönelik Citi Gereklilikleri ("**Gereklilikler**"), Tedarikçilerin Citi ile iş yaparken yerine getirmeleri gereken yükümlülüklerden bazılarını ayrıntılı olarak açıklamaktadır. Belirli Gereklilikler tüm Tedarikçiler için geçerlidir; ancak diğer Gerekliliklerin belirli bir Tedarikçi için geçerliliği, Tedarikçinin Citi'ye sağladığı ürünler ve hizmetlerin türlerine bağlıdır (ikincisi aşağıdaki Bölüm 1.2'de özetlenmiştir ve burada listelenen her hükmün başında belirtilmiştir). Büyük harfle yazılan terimler, ilişikteki Ek de dâhil olmak üzere, burada kendilerine atfedilen anlamlara sahip olacaktır; ancak burada böyle bir anlam belirtilmemişse, aşağıda tanımlandığı şekliyle Sözleşmede kendilerine atfedilen anlamı taşıyacaktır.

Bu Gereklilikler, Citi ile yapılan Tedarikçi sözleşmeleri (iş emirleri, lisans programları gibi işlem belgeleri dâhil ancak bunlarla sınırlı olmamak üzere) kapsamındaki sözleşmeye dayalı yükümlülüklerdir (her biri bir "**Sözleşme**") ve herhangi bir Sözleşmede belirtilen yükümlülüklerle, Yürürlükteki Yasa kapsamındaki yükümlülüklerle (bu terimin aşağıda tanımlandığı gibi), Tedarikçiye aynısı kapsamındaki yükümlülüklerini bildiren Citi'den Tedarikçiye herhangi bir bildirim (her biri bir "**Bildirim**") veya Citi'nin işletmeleri veya işlevleri tarafından uygulanan daha spesifik ek gerekliliklere ilave niteliğindedir. Yukarıdaki gerekliliklerden herhangi biri ile bu gereklilikler arasında herhangi bir çelişki olması durumunda, daha kısıtlayıcı olan yükümlülükler ve gereklilikler geçerli olacaktır. Tedarikçiler proaktif bir rol üstlenmeli ve bu Gerekliliklerdeki herhangi bir değişiklik, bu Gerekliliklerde talep edilen muafiyetler ve bu Gerekliliklerdeki veya Yürürlükteki Yasalarla herhangi bir algılanan uyumsuzluk dâhil olmak üzere, bu Gerekliliklerle ilgili soruları için birincil Citi iş irtibatlarına (veya onun görevlendirdiği kişiye) danışmalıdır.

Tedarikçi, Citi'nin Geçerli Yasaya uyma yükümlülüğü ile bağlantılı olarak Tedarikçi Hizmetleri veya Personeli ile ilgili olarak talep ettiği veriler için Citi'nin Tedarikçiye gönderebileceği her türlü makul talebi derhâl yerine getirecektir. Tedarikçinin bu yükümlülüklerle uymaması, bu Sözleşmenin şartlarının esaslı ihlali olarak kabul edilecektir.

Bu Gerekliliklere veya Tedarikçinin iş yaptığı bir Citi işletmesi tarafından belirtilen herhangi bir ek gerekliliğe uyulmaması, bir Tedarikçinin Citi ile olan Sözleşmesinin feshedilmesine neden olabilir. Ayrıca, Gerekliliklerin ihlali aynı zamanda Yürürlükteki Yasanın da ihlali olabilir ve Citi'ye (veya üçüncü taraflara) ödenecek hukuki tazminata ya da Tedarikçiye uygulanacak cezai yaptırımlara yol açabilir. Tedarikçi, bu Gerekliliklerin herhangi bir hükmüne uygun olmak zorunluluğunun yerine, kendi politikaları ile uyumluluğu, Citi'nin yazılı onayı olmaksızın kullanamaz.

1.2. Seçilmiş Tedarikçiler için Geçerli Gereklilikler

Aşağıdaki tabloda, burada belirtilen uygulanabilirlik kriterlerini karşılayan belirli Tedarikçilere uygulanan belirli Gereklilikler listelenmektedir. Aşağıda belirtilmeyen bölümler TÜM Tedarikçiler için geçerlidir.

Bölüm No.	Bölüm Başlığı	Uygulanabilirlik
2	EŞİT İSTİHDAM FIRSATI/POZİTİF AYRIMCILIK	Citi'nin ABD federal hükûmeti ile yaptığı bir sözleşmenin ifası için gerekli olan sözleşmelere ve satın alma siparişlerine uygulanır; söz konusu sözleşmenin veya satın alma siparişinin bir federal hükûmet alt sözleşmesi veya satın alma siparişi teşkil edip etmediği hususunda belirsizlik olması hâlinde, uygunluğuna göre maddenin başına veya sonuna "Uygun olduğu şekilde" ifadesini ekleyin.
12	KARA PARA AKLAMA İLE MÜCADELE	Müşteriyle ilgili belirli hizmetlerin yerine getirilmesi (ör., müşteri kabulü, müşteri hesabı ve işlem taraması) veya yukarıda söz edilen aktivitelerle ilgili verileri/ölçümleri sağlayan Tedarikçiler için geçerlidir; <u>VE/VEYA</u> Nakit veya finansal araçlarla ilgili olarak aracı görevi gören Tedarikçiler (ör., uzaktan çek yatırma, kurye, zırhlı araç veya Lockbox tahsilat hizmetleri).
13	KAYIT YÖNETİMİ	Citi Bilgilerine erişen/işleyen/depolayan Tedarikçiler için geçerlidir
14	İŞ DEVAMLILIĞI	Citi tarafından kullanılan hizmetleri sağlayan veya teknoloji altyapısını/uygulamalarını barındıran Tedarikçiler için geçerlidir. Citi Ticari Aktivite Sahibi (BAO), uygulanabilirliği ve COB gerekliliklerini Tedarikçiye iletmekten sorumludur.
15	GLOBAL ARKA PLAN TARAMASI STANDARTLARI	Citi'ye hizmet sağlayan Tedarikçiler için geçerlidir.
16	GİDERLER	Sözleşmeye bağlı olarak geri ödenebilir işletme masrafları talep etmeye uygun Tedarikçiler için geçerlidir.
17	BİLGİ GÜVENLİĞİ (İS)	Citi Bilgilerine erişen/bunları işleyen/yöneten/depolayan <u>VE/VEYA</u> Citi markalı internete dönük uygulamalar için bir Ana Sistem olarak sorumlu olan Tedarikçiler <u>VE/VEYA</u> Citi'nin ağ kaynaklarına bağlantısı olan Tedarikçiler <u>VE/VEYA</u> Citi tesislerine refakatçisiz erişime ihtiyacı olan Alt Yükleniciler de dâhil olmak üzere Tedarikçiler için geçerlidir.
18	GÜVENLİ İŞ YERİ KURALLARI	
19	YAPAY ZEKÂ/MAKİNE ÖĞRENİMİ (Üretken Yapay Zekâ/Ajan Yapay Zekâ dâhil)	Citi tarafından tanımlandığı şekliyle, sağladıkları ürünün/hizmetin herhangi bir bölümünde Yapay Zekâ/Makine Öğrenimi (AI/ML) kullanan Tedarikçiler için geçerlidir.
20	KİŞİSEL TİCARET VE YATIRIM POLİTİKASI	Citi'deki iş sorumluluklarının bir parçası olarak MNPI'ye düzenli erişim gerektiren Tedarikçiler için geçerlidir.
23	ZORUNLU UZAKLAŞTIRMA POLİTİKASI	Bu Politika, Hassas Pozisyonlarda (Sözlükte tanımlandığı şekliyle) bulunan Çalışan Olmayan Personel ("Çalışanlar") ("Hassas Çalışanlar"), Hassas Çalışanların doğrudan yöneticileri ve amirleri ("Yöneticiler") ve Hassas Çalışan Olmayan Personelin Citi İş İrtibat Kişileri için geçerlidir.

2 EŞİT İSTİHDAM FIRSATI

2.1 Eşit İstihdam Fırsatı.

Citi; ırk, renk, din, cinsiyet, cinsel yönelim, cinsiyet kimliği, ulusal köken, vatandaşlık, göçmenlik durumu, yaş, medeni durum, genetik bilgiler, engellilik, korunan gazilik durumu veya yasalarca korunan herhangi başka bir özellik dikkate alınmaksızın tüm vasıflı kişilere eşit istihdam fırsatları sağlamak üzere tasarlanmış olan politikaları geliştirmiştir.

Tedarikçiler, Citi'nin Tedarikçiye uyması gerektiğini yazılı olarak bildirdiği bu tür yasa veya yönetmelikler dâhil ancak bunlarla sınırlı olmamak üzere, tüm geçerli ayrımcılık yapmama yasaları ve regülasyonlarının gerekliliklerine uyacak ve personelinin bunlara uymasını sağlayacaktır.

Tedarikçiler, www.citigroup.com/global/eeo-aa-policy adresinde bulunabilecek ABD Eşit İstihdam Fırsatı Politikası Bildirimini inceleyecek ve buna uygun eylemi gerçekleştirecektir.

2.2 Devlet Sözleşmeleri

Federal hükûmetle yapılan bir Citi sözleşmesinin yerine getirilmesi için gerekli olan sözleşmeler ve satın alma siparişleri, aşağıda gösterildiği gibi kalın harflerle yazılmış aşağıdaki maddeyi kelimesi kelimesine içermelidir. (Bunun bir federal hükûmet alt sözleşmesi/satın alma emri olup olmadığından emin değilseniz, ekleme yönünde hareket edin ve bölümün başına "Uygun olduğu şekilde" ifadesini ekleyin).

[Uygun olduğu şekilde,] Tedarikçi, geçerli tüm Federal ayrımcılık karşıtı yasalara uyacak ve geçerli herhangi bir Federal ayrımcılık karşıtı yasayı ihlal eden herhangi bir program işletmediğini beyan eder

2.3 Devlet Sözleşmeleri Eki

Federal hükûmetle yapılan bir Citi sözleşmesinin yerine getirilmesi için gerekli olan sözleşmeler ve satın alma siparişleri, alt sözleşme veya satın alma siparişinin ekinde aşağıdaki bildirim içermelidir. (Bunun bir federal hükûmet alt sözleşmesi/satın alma emri olup olmadığından emin değilseniz, aşağıdaki bildirim ekleyin ve "Uygun olduğu şekilde" ifadesini aşağıdaki bildirimin sonuna ekleyin.)

Bir federal hükûmet yüklenicisi olarak Citigroup, aşağıda imzası bulunan yükleniciye veya satıcıya, korunan gaziler ve engelli bireyler adına eşit istihdam fırsatı yükümlülüklerimiz hakkında yazılı bildirimde bulunmaktadır. Citigroup, Section 503 of the Rehabilitation Act ve Vietnam Era Veterans' Readjustment Assistance Act ile bunlara ilişkin sırasıyla 41 C.F.R. § 60-741 ve 41 C.F.R. § 60-300 kapsamındaki geçerli regülasyonlara tamamen uyar. Eşit İstihdam Fırsatı Politika Bildirimimizi www.citigroup.com/global/eeo-aa-policy adresinde bulabilirsiniz. EEO Politika Bildirimimiz ile ilgili her türlü sorunuzu Politika Bildirimimizde belirtilen kişiye yönlendirebilirsiniz.

[Uygun olduğu şekilde], Politika Bildirimimiz ve regülasyonlarla tutarlı olarak uygun eylemi gerçekleştirmenizi rica ediyoruz..

3 RÜŞVET VE YOLSUZLUKLA MÜCADELE (AB&C)

Citi, geçerli AB&C yasalarına uymak için makul şekilde tasarlanan politikalar, prosedürler ve iç kontrollere sahiptir ve herhangi bir biçimde rüşvet veya kolaylaştırma ödemelerini kesinlikle yasaklar. Tedarikçiler (İş Tanıtıcıları dâhil), bunların Personeli veya doğrudan ya da dolaylı olarak Citi adına hareket eden kişiler, faaliyetlerini en yüksek etik standartlara uygun olarak ve her biri tadil edilmiş hâliyle U.S. Foreign Corrupt Practices Act (FCPA), U.K. Bribery Act (UKBA) ve Citi'nin faaliyet gösterdiği ülkelerde geçerli diğer tüm yerel AB&C yasalarına uygun biçimde yürütecektir.

Tedarikçi ve Citi adına veya Tedarikçinin Citi ile yaptığı herhangi bir sözleşme ya da ilişkiyle bağlantılı olarak faaliyet gösteren Personelinden hiçbirisi, (i) herhangi bir kişiye ödeme, menfaat, avantaj veya değer taşıyan başka herhangi bir şey vermeyecek, sağlamayacak, bunlara izin vermeyecek ya da bunları teklif etmeyecek; veya (ii) herhangi bir kişiden ödeme, menfaat, avantaj veya değer taşıyan başka herhangi bir şeyi almayacak ya da kabul etmeyecektir; (i) ve (ii) kapsamındaki her durumda FCPA, UKBA veya diğer AB&C yasaları ihlal edilmemelidir. Tedarikçi ve Personeli, Citi adına veya Tedarikçinin Citi ile yaptığı herhangi bir anlaşma veya ilişkiyle bağlantılı aktivitelerini ve işlemlerini, bu Bölüm de dâhil olmak üzere Gerekliliklere uygun olarak yürütmelidir. Tedarikçi ve Personeli aynı zamanda bir AB&C uyumluluk programını ve tüm AB&C yasalarına uygunluğunu sağlamak için tasarlanmış ve uygulanan politika ve prosedürleri de sürdürmelidir.

Citi'nin AB&C Program'ına genel bakış için lütfen [Citigroup's Investor Relations](#) sayfasını ziyaret edin (Citi Policies altında AB&C Program'ı seçin).

4 HEDİYELER VE AĞIRLAMA

Tedarikçiler veya Personeli; bunun fiilî ya da görünürde bir çıkar çatışması veya karşılık ilişkisi yaratacağı, çalışanın dürüstlüğüne ya da muhakemesini zedeleyeceği, çalışanın kararlarını başka bir şekilde uygunsuz olarak etkileyeceği, çalışanı görevlerine aykırı davranmaya yöneltceği veya yürürlükteki yasaları başka bir şekilde ihlal edeceği durumlarda Citi çalışanlarına hediye ya da değer taşıyan herhangi bir şey (ağırlama dâhil) veremez. Yukarıda belirtilenleri sınırlamaksızın çalışan, G&E Standard'ın Prohibited Gifts and Entertainment Section bölümüne uymalıdır. Tedarikçiler ve Personeli, herhangi bir Citi çalışanına takvim yılı başına kişi başı toplam 300 ABD dolarını aşan nakit dışı iş hediyeleri vermemelidir.

Bir Tedarikçi bir Citi çalışanına iş amaçlı ağırlamayı (ör., bir yemek, spor, kültür veya diğer karşılaştırılabilir etkinlik) sağladığında, Tedarikçi etkinliğe katılmalıdır ve ağırlama uygun, alışılmış ve makul olmalı, abartılı veya aşırı derecede sık olmamalıdır. Ayrıca, Tedarikçi etkinlikte hazır bulunmuyorsa ağırlama bir iş hediyesi olarak kabul edilecek ve Citi Gifts and Entertainment Standard kapsamında geçerli raporlama eşiklerine tabi olacaktır. Tedarikçi; bunu yapmanın yolsuzluk niteliğinde, uygunsuz veya yürürlükteki yasaya aykırı olacağı ya da makul olarak böyle algılanacağı durumlarda, masrafı Tedarikçiye veya bir Citi çalışanına ait olsa dahi, Citi adına veya sözde Citi adına doğrudan ya da dolaylı

olarak herhangi bir kişiye değer taşıyan hiçbir şey veremez ve başka bir kişiyi de bunu yapmaya teşvik edemez.

5 TEDARİKÇİ KATILIMI VE TEDARİKÇİ İLKELERİ

<https://www.citigroup.com/citi/suppliers/>Citi, Tedarikçilerle çeşitli girişimlerde bulunur ve hizmet verdiğimiz topluluklardan potansiyel Tedarikçiler ile Citi'nin satın alma programı hakkında farkındalık yaratmak için çalışır. Bu katılımlar ayrıca, özellikle ortaya çıkan iş sorunlarına yönelik yenilikçi çözümler üreten gelecek vaat eden Tedarikçileri belirlemeyi amaçlamaktadır. Citi'nin Tedarikçilere yönelik beklentileri hakkında ek bilgiler [Doing Business with Citi](#) sitesinde aşağıdaki başlıklar altında yer almaktadır:

[Citi Statement of Supplier Principles](#)
[Citi Sustainable Progress Strategy](#)

6 MODERN KÖLELİĞİN YASAKLANMASI

Citi, kendi kuruluşunda veya tedarik zincirlerinde modern kölelik ve insan ticareti yaşanması riskini belirlemeyi ve önlemeyi amaçlayan uygulamaları sürdürme taahhüdündedir. Citi'nin Tedarikçileri, aşağıda belirtilen Gerekliliklere uyacak ve kendi operasyonlarında ve tedarik zincirlerinde modern kölelik ve insan ticareti riskini belirlemek ve önlemeye çalışmak üzere kuruluş genelinde etkili politikalar, prosedürler ve/veya uygulamalar geliştirecektir. Tedarikçilerin, Citi'nin özellikle yüksek riskli sektörler ve coğrafyalardaki Tedarikçiler için riske maruz kalma ve potansiyel azaltma adımlarını değerlendirmesine olanak sağlamak için Citi'nin talebi üzerine, gerektiği gibi ek bilgiler dâhil olmak üzere, Citi'nin Kurumsal Sorumluluk Anketini doldurmaları gerekmektedir. Tedarikçinin alt yüklenicilerinin de aynı süreci takip etmesi beklenmektedir.

6.1 Çocuk İş Gücünden Kaçınma

Tedarikçiler çocuk işçi çalıştırmayacaktır. “Çocuk” terimi, yürürlükteki yasalar uyarınca asgari çalışma yaşının altındaki kişiyi veya bu tür yasaların bulunmaması hâlinde 15 yaşın ya da zorunlu eğitimi tamamlama yaşının altında olan kişiyi (hangisi daha yüksekse) ifade eder. Çocuk işçiliğinin kullanılmasına ilişkin üstün yasağa tabi olarak, 18 yaş altındaki işçiler çalıştırılıyorsa, bu işçilerin yaptıkları görevler ve çalışma koşulları konusunda, çalışmalarının veya çalışma koşullarının doğrudan veya dolaylı bir sonucu olarak fiziksel, ruhsal veya başka bir zarara uğramamalarını sağlamak için özel bir özen gösterilmelidir.

6.2 Serbestçe Seçilen İş

Tedarikçi; çalışanların zorlanmamasını, zihinsel veya fiziksel baskıya maruz bırakılmamasını, borç karşılığı ya da sözleşmeyle bağlı çalıştırılmamasını, gönüllü olmayan cezaevi işçiliğine veya kölelik amacıyla insan ticaretine maruz bırakılmamasını ve zorunlu fazla mesai dâhil herhangi bir biçimde cebri çalışmaya tabi tutulmamasını sağlamalıdır. Tüm iş gönüllü olarak yapılmalıdır. Tedarikçinin işbu sözleşme kapsamındaki yükümlülükleri, aşağıdakileri sağlamayı içerir ancak bunlarla sınırlı değildir:

1. **Sözleşmeler, Ücretler ve Çalışma Saatleri:** Çalışanların çalışma veya görevlendirme şartları, kendileri tarafından kolayca anlaşılabilir ve hak ve yükümlülüklerini açıkça belirten yazılı bir belgede belirtilir. Bu yazılı belge, ücretler, fazla mesai ücreti, ödeme dönemleri, çalışma saatleri ve dinlenme molaları ve tatil hakları ile ilgili şeffaf şartları içerecek, ancak bunlarla sınırlı olmayacaktır. Bu tür yazılı şartlar, işe başlamasından önce işçiye bildirilecek, işveren tarafından dikkate alınacak ve işin yapıldığı yerdeki endüstri standartlarını ve geçerli yasaların ve toplu sözleşmelerin asgari gerekliliklerini karşılayacaktır.
2. **Çalışmayı Serbestçe Sonlandırma Hakkı:** Çalışanlar, yürürlükteki yasalar ve toplu sözleşmeler uyarınca makul bir ihbar süresinden sonra ve herhangi bir uygunsuz cezaya çarptırılmadan, uygun şekilde iş sözleşmelerini serbestçe feshetme hakkına sahip olmalıdır.
3. **İnsanlık Dışı Muamele:** Çalışanlar, aileleri ve onlarla yakın ilişki içinde olanlar, fiziksel cezalandırma, fiziksel, psikolojik veya cinsel şiddet veya zorlama, sözlü taciz, taciz veya korkutma dâhil ancak bunlarla sınırlı olmamak üzere sert veya insanlık dışı muameleye tabi tutulamazlar. Göçmen işçiler, aileleri ve onlarla yakın ilişki içinde olanlar, uyrukları nedeniyle çalışma şartları ve koşullarında ayrımcılığa maruz bırakılmamalıdır.
4. **Ücretler, Yan Haklar ve Çalışma Saatleri:** Tazminat, asgari ücret, fazla mesai saatleri ve yasal olarak zorunlu yan haklar dâhil olmak üzere geçerli tüm ücret yasalarına uygun olmalıdır. Çalışanların ücretleri tam ve zamanında ödenmeli ve kendilerine şeffaf ücret bordroları sunulmalıdır. Disiplin tedbiri olarak ücretlerden veya yan haklardan cezalandırıcı nitelikte kesinti yapılamaz ya da bunlar alıkonulamaz. Haftalık çalışma süreleri yerel mevzuatın belirlediği azami sınırı aşmamalıdır; fazla çalışma gönüllülük esasına dayanmalı, yasal sınırlar dâhilinde kalmalı ve fazla çalışmayı reddetmek cezalandırılmamalıdır.
5. **Kimlik Belgelerine El Konulmaması:** Çalışanların kimlikleri, seyahat izinleri, pasaportları veya diğer resmî belgeleri veya diğer değerli eşyaları, istihdam koşulu olarak müsadere edilemez veya alıkonulamaz ve malların alıkonulması, doğrudan veya dolaylı olarak çalışanların özgürlüklerini kısıtlamak veya iş yerinde kölelik yaratmak için kullanılamaz.
6. **İşe Alım Ücreti veya Borç Esareti Olmaması:** Çalışanların işe alınmasıyla ilgili ücretler veya masraflar (çalışma vizeleri, seyahat masrafları ve belge işleme masrafları dâhil ancak bunlarla sınırlı olmamak üzere) doğrudan veya dolaylı olarak çalışanlara yansıtılmayacaktır. Benzer şekilde, işçilerden, güvenlik ödemeleri de dâhil olmak üzere iş yerinde kölelik yaratma amacı veya etkisi olan ödemeler yapmaları ya da borçlarını iş yoluyla ödemeleri istenmeyecektir. İşçilere işe alım süreciyle ilgili olarak ücret veya masraflar yansıtıldığı veya bunların istihdam sırasında ortaya çıktığı tespit edilirse, Tedarikçi bu masrafların hemen geri ödenmesini sağlamak için makul önlemleri alacaktır.

İşçilerin, istihdam bürosu gibi üçüncü bir taraf aracılığıyla işe alınmasının gerekli olduğu durumlarda, yalnızca saygın istihdam büroları işe alınacaktır. İşçilerin doğrudan istihdam edilmek üzere temin edilmesi durumunda, yalnızca saygın işe alım ajansları ile çalışılacaktır. İşe alım ücretlerinin çalışanlar tarafından ödenmesi yasağı tüm işe alım uzmanları, acenteler ve alt acenteler için geçerlidir. Tedarikçiler, uyumu sağlamak için kontrollere sahip olacaktır. **Hareket Özgürlüğü:** Çalışanlar, makul olmayan kısıtlamalara tabi olmaksızın hareket etme özgürlüğüne sahip olacak ve fiziksel olarak iş yerine veya işverenin kontrolündeki diğer yerlere (örneğin, konaklama blokları) hapsedilmeyecektir. Çalışanların, işin yeri veya doğası gereği gerekli olduğu durumlar haricinde, işverenin kontrolündeki iş yerlerinde konaklama yapmaları yönünde bir zorunluluk getirilmeyecektir.

- 7. Misilleme yapılmaksızın şikâyetler:** İşçiler, işverenlerine işverenin kendilerine yönelik muamelesi hakkında mağduriyetlerini bildirmekte serbest olacak ve işçiler bir mağduriyetin bildirilmesinden dolayı zarar, misilleme veya mağduriyet yaşamayacaktır.

7 TEDARİKÇİ PERSONELİ

7.1 Tedarikçi Personel Eğitimi, Atama, Yeniden Atama ve Yönetimi

Tedarikçi, Hizmetleri herhangi bir Sözleşmeye uygun olarak en etkili şekilde yerine getirmek için uygun eğitim, öğretim, deneyim ve beceriye sahip yeterli sayıda kişiyi kullanacak ve talep üzerine bu kişilerin niteliklerini kanıtlayacaktır. Personel bir Projeye atandıktan sonra Tedarikçi, Citi'nin önceden yazılı onayı olmadan Proje üzerinde çalışma olanağını azaltacak şekilde herhangi bir Personeli yeniden görevlendirmeyecek veya başka konularda kullanmayacaktır ve genel olarak Personeli, yeniden oryantasyon ihtiyacından kaynaklanan kesintileri en aza indirecek şekilde Projelere atayacaktır. Tedarikçi, Personelinin kendilerini Citi'nin çalışanı veya temsilcisi olarak tanıtmamasını veya Citi tarafından sağlanan yan haklara hak kazanma veya engellilik geliri, sosyal güvenlik vergileri veya yardımları, Federal işsizlik vergileri, Eyalet işsizlik sigortası yardımları veya Federal gelir vergisi stopajı dâhil olmak üzere herhangi bir amaçla Citi'nin çalışanı olarak muamele görmeyi talep etmemesini sağlayacaktır. Tedarikçi, gerekli tüm sigorta teminatlarını sürdürmek, geçerli tüm vergi beyannamelerini doldurmak ve gerekli tüm ödemeleri ve vergi mevduatlarını Tedarikçinin bağımsız bir yüklenici statüsüyle tutarlı bir şekilde yapmak dâhil, ancak bunlarla sınırlı olmamak üzere, Personeli ile ilgili olarak tüm işverenle ilgili sorumluluklardan tek başına sorumludur.

7.2 Tedarikçi Personelinin Değiştirilmesi

Tedarikçi tarafından bir Projeye atanan herhangi bir Personelin diğer herhangi bir ayrımcı olmayan nedenle Citi tarafından kabul edilemez olduğunun Citi tarafından Tedarikçiye bildirilmesi durumunda, Tedarikçi, söz konusu personeli çıkaracak ve değiştirecektir. Tedarikçi ayrıca, bir Projeye atanan herhangi bir Personelin Hizmetleri zamanında ve profesyonel bir şekilde sunmadığı veya sunmak istemediği durumda söz konusu Personeli çıkarmayı ve değiştirmeyi ve Citi'ye Hizmet sunmaktan (veya Hizmetlerin teslimi veya gözetimi ile ilgili herhangi bir sorumluluktan) derhâl men etmeyi kabul eder.

7.3 Tedarikçinin Personel Politikaları

Tedarikçi; gerçek kişi olan ve Citi'ye yerinde Hizmet sağlamak üzere görevlendirilen Personelinin uygunluğunu belirlemeye yönelik kapsamlı politika ve prosedürleri sürdürdüğünü ve etkili biçimde uyguladığını ve bu politika ve prosedürlerin, Yürürlükteki Yasa ve geçerli toplu iş sözleşmesinin izin verdiği ölçüde, çalışma izni doğrulamasını, burada ayrıca belirtildiği üzere istihdam geçmişi ve cezai mahkûmiyetlere ilişkin geçmiş kontrollerini ve işe giriş öncesi uyuşturucu testini içerdiğini beyan, garanti ve taahhüt eder. Yukarıdakilerin genel geçerliliğini sınırlamaksızın, Tedarikçi ayrıca, Tedarikçinin tüm göçmenlikle ilgili Uygulanabilir Yasalara tam olarak uymasını sağlamak için kontrollere ve prosedürlere sahip olduğunu beyan, garanti ve taahhüt eder; bu, Citi'ye atanan tüm Tedarikçi Personelinin görevlendirme boyunca tüm göçmenlikle ilgili Uygulanabilir Yasalara tam olarak uygun şekilde çalışmaya yetkili olduğunu doğrulamayı da içerir. Talep üzerine Tedarikçi, Citi'ye atanan Tedarikçi Personelinin herhangi biri veya tümü için çalışma izninin yazılı kanıtını ve göçmenlikle ilgili Yürürlükteki Yasalara uygunluğunun yazılı kanıtını derhâl Citi'ye sunacak ve Hizmetlerin zamanında ve etkin bir şekilde sağlanmasını sağlamak için gerekli tüm eğitim ve oryantasyonu sağlamak dâhil olmak üzere, her durumda Citi'ye hiçbir ek ücret ödemedi, yürürlükteki Yasa ile uyumlu çalışma iznine sahip olmayan tüm Personeli uygun niteliklere sahip personelle değiştirecektir.

7.4 Tedarikçi Sahipliği

Citi'nin iş yaptığı yargılama alanlarında geçerli yasa ve regülasyonlara uymak amacıyla, Citi'nin talebi üzerine, Tedarikçiler, Tedarikçinin birinci derece sahipleri de dâhil olmak üzere ve sözleşme, ürün veya hizmet üzerinde etki veya başka yollarla doğrudan veya dolaylı olarak mülkiyete veya kontrole sahip olan nihai intifa hakkı sahibine kadar olan hak sahibini kapsayacak şekilde gerçek kişi ve/veya kuruluş olan sahiplerin bilgilerini sağlamakla yükümlüdür.

8 DOLANDIRICILIK YÖNETİMİ

Citi'nin dolandırıcılık riskini belirleme ve azaltma çabalarıyla bağlantılı olarak ("Dolandırıcılık Yönetimi").

8.1 Tüm Tedarikçiler:

1. Şüpheli veya iddia edilen hırsızlık, dolandırıcılık veya diğer olası suç aktivitesi veya görevi kötüye kullanma ile ilgili tüm Citi soruşturmalarında ve dolandırıcılık veya suç teşkil eden davranışların kovuşturulmasında yasaların izin verdiği ölçüde iş birliği yapacaktır;
2. Herhangi bir potansiyel dolandırıcılık vakasının [Ethics Hotline](#) üzerinden Citi'ye zamanında raporlanmasını ve yönlendirilmesini sağlayacaktır. Bu kapsam; Citi, bir Citi çalışanı, bir Citi Tedarikçisi veya temsilcisi ya da Citi çalışanı olmayan personel (ör., geçici çalışanlar ve yükleniciler) ile ilgili teşebbüs edilmiş, şüphelenilen, iddia edilen veya fiilen gerçekleşmiş hırsızlık ve dolandırıcılık (ör., Tedarikçi hakkında bilerek yanlış, hatalı veya yanıltıcı veri sunulması, faturalandırma düzenleri, fonların veya menkul kıymetlerin kaybolması vb.), suç aktivitesini veya görevi kötüye kullanmayı içerir ancak bunlarla sınırlı değildir.

3. Citi ve temsilcilerinin izleme ve gözetimine izin vermek ve söz konusu Tedarikçiyi ilgilendiren olası dolandırıcılık aktivitelerine yönelik Citi veya kolluk kuvvetleri öncülüğündeki soruşturmaları desteklemek.
4. Tedarikçilerin haberdar edildiği çıkar çatışmalarını (Tedarikçiler/Tedarikçinin Çalışanları ve/veya Citi Çalışanları arasındaki çıkar çatışmaları dâhil) zamanında bildirmek; ve
5. Citi'nin Tedarikçi ödeme sisteminde bir Tedarikçinin banka hesabının açılması veya güncellenmesi sırasında Citi'nin dolandırıcılık önleme süreçlerini desteklemek.

8.2 Buna ek olarak, dolandırıcılık riskine doğası gereği daha açık olan hizmetler sunan Tedarikçinin şunları yapması **gerekir**:

1. Citi'ye sağladıkları hizmetlerle ilgili önemli dolandırıcılık risklerini ve bu riskleri azaltmak için yürürlükte bulunan kontrolleri ve prosedürleri belirleyen bir Fraud Risk Management Program'ı belgelemek ve uygulamak.
2. Dolandırıcılık farkındalığı eğitimini tamamlamak (işe alındıktan sonraki 90 takvim günü içinde ve sonrasında her yıl) ve personeli Citi'ye sağlanan belirli hizmetlerle ilgili dolandırıcılık riskinin belirli unsurları konusunda eğitmek.
3. Dolandırıcılık girişimi vakalarını izlemek ve Citi'ye sağladıkları hizmetlerle ilgili dolandırıcılık riskini en aza indirmek için etkili kontrolleri devam ettirmek, kontrol prosedürlerini belgelemek ve kontrollerin etkililiğini düzenli olarak test ederek, tüm eksiklikleri Ticari Aktivite Sahibine (BAO) raporlamak.
4. Durum tespiti/dolandırıcılık riskine maruz kalmanın sürekli izlenmesi/değerlendirilmesi için Ticari Aktivite Sahibine (BAO) gerekli her türlü bilgiyi sağlamak
5. Durum Tespiti, Tedarikçilerin dolandırıcılık riskini azaltmaya ilişkin yeteneklerinin kontrol değerlendirmelerini gerçekleştirmek üzere tasarlanmış Üçüncü Taraf Dolandırıcılık Etki Değerlendirme Şablonu'nu ("TP-FIAT") içerir. Bu işletme prosedürü, Ticari Aktivite Sahibi (BAO) veya Üçüncü Taraf Görevlisi (TPO) ve Dolandırıcılık Risk Yönetimi Görevlisi ("FRMO") tarafından dolandırıcılık riskini belirlemek ve yönetmek için gerçekleştirilecek bir dizi adımı açıklamaktadır.

8.3 Doğası gereği daha yüksek dolandırıcılık riskine sahip olan tedarikçiler aşağıdaki durumlardakiler olup yalnızca bunlarla sınırlı değildir:

1. Citi'nin doğrudan kontrolü veya denetimi altında olmadığına, dâhilî hesaplara, finansal işlemlere, nakit işlemlerine erişim gibi dolandırıcılık amacıyla kullanılacak Gizli veya daha yüksek gizlilik derecesi olarak sınıflandırılan verilere erişim hakkına sahip olmak.
2. Citi ağlarına/sistemlerine bağlantıya sahip olmak; ve
3. dolandırıcılık yapmak veya dolandırıcılığa olanak sağlamak amacıyla hedeflenebilecek hizmetleri ve yetenekleri sağlamak, desteklemek veya bunlara erişim sağlamak, bunlar arasında şunlar yer alır:

- a) Yeni müşterilerden gelen başvuruların belirlenmesi, sisteme dâhil edilmesi veya işlenmesi.
- b) Citi veya Müşteri Ödeme/Fon Transferi aktiviteleri ve/veya Citi müşterilerinin bu hizmetlere erişiminin doğrulanması;
- c) Citi verilerinde veya Citi müşterisinin (ör., demografik) verilerinde değişiklik yapma, değişiklikleri kontrol etme veya giderme;
- d) İşlem araçlarının (ör., bankamatik/kredi kartları, e-Cüzdanlar, çek defterleri, vb.) sağlanması, bakımı veya yetkilendirilmesi;
- e) Dolandırıcılık olaylarının önlenmesi, saptanması veya yanıtlanması ile bağlantılı olarak, Citi'ye işlemsel dolandırıcılık yönetimi aktivitelerinin sağlanması veya Citi'nin bu aktivitelerde desteklenmesi;
- f) Nakit, finansal araçlar ve varlıklara/fiziksel mallara fiziksel erişim sağlanması;
- g) Citi tesislerine refakatsiz veya mesai saatleri dışında erişim;
- h) Finansal Tablolar: GL/SL'ye girişlerin kaydedilmesi gibi muhasebe aktiviteleri;
- i) Teşvik edilmiş aktiviteler için Ödüller kazanılması ve harcanması.

9 MEDYA ETKİLEŞİMİ VE KAMUOYUNUN ÖNÜNE ÇIKMA

Citi Kurum Hizmetleri ve Halkla İlişkiler, Citi adına basın veya kamuoyu açıklamalarını yayımlama yetkisine sahip olan tek departmandır. Tedarikçiler, doğrudan veya dolaylı olarak Citi'yi, bir Tedarikçi ve Citi arasındaki herhangi bir Sözleşmeyi veya düzenlemeyi veya Citi tarafından bir Tedarikçiden satın alınan ürünleri ve hizmetleri tanımlayan herhangi bir basın açıklamasını yayımlayamaz. Tedarikçiler, Citi ile ilgili olarak Müşteriler, Citi çalışanları, diğer Citi Tedarikçileri, Tedarikçilerin diğer müşterileri veya herhangi bir üçüncü tarafla, birincil Citi iş irtibat kişisinin önceden yazılı onayı olmaksızın herhangi bir halkla ilişkiler faaliyetine izin veremez veya bu tür faaliyetlerde bulunamaz.

Tedarikçiler, Citi'den, Citi'nin faaliyetlerinden, Müşterilerden, ürünlerden veya hizmetlerden bahseden yazılı veya elektronik formatta hiçbir materyali (kitaplar, makaleler, podcast'ler, web yayınları, bloglar, web sitesi gönderileri, fotoğraflar, videolar, sosyal medya veya diğer medya dâhil) yayımlayamaz veya gönderemez, konuşma yapamaz veya röportaj veremez veya kamuya açık görünümde bulunamaz; bunun için birincil Citi iş irtibat kişisinden ve kıdemli ülke halkla ilişkiler görevlisinden önceden yazılı onay almalıdır.

Tedarikçiler, Citi'ye hizmet veya ürün sağlanmasıyla bağlantılı olsun veya olmasın, Citi'nin tescilli işaretlerini, ticari markalarını, hizmet markalarını, ticari adlarını, logolarını, sembollerini veya marka adlarını, her durumda Citi'nin önceden yazılı onayını almadan kullanamazlar. Tedarikçiler, Citi'nin adını, logosunu veya ticari markalarını, tesislerini veya ilişkilerini Citi dışındaki bir çıkar veya iş için (antetli kâğıtlarda veya kişisel web sitelerinde, bloglarda veya diğer sosyal ağ sitelerinde dâhil) kullanamazlar. Ayrıca, Tedarikçiler Citi'nin adını, tesislerini veya ilişkilerini hayır amaçlı veya karşılıksız yapılan hizmetler için kullanamaz.

10 YAZILI ELEKTRONİK İLETİŞİMLER

Citi personeliyle etkileşim kurarken veya Citi namına veya adına yükümlülüklerini yerine getirirken, Tedarikçilerin yalnızca Citi tarafından onaylanmış Yazılı Elektronik İletişim Ekipmanları, Sistemleri ve Hizmetleri kullanmalarına izin verilir. Bağımsız araçlar olarak ya da daha geniş bir platforma entegre edilmiş biçimde, Citi tarafından veya üçüncü tarafça sağlanan yeni, genişletilmiş veya değiştirilmiş Citi eComm Channels, BAO tarafından Tedarikçiye yazılı olarak bildirilen geçerli Citi Gerekliliklerine uygun şekilde onaylanmalıdır. Citi personeli ile WhatsApp, WeChat, LINE, Slack, Signal, Telegram, iMessage, SMS, Viber ve diğer interaktif elektronik platform gibi Citi tarafından onaylı olmayan mesajlaşma platformları üzerinden Citi işleri konusunda iletişim kurmak yasaktır.

Ayrıca, Tedarikçiler, Citi tarafından sağlanan İletişim Ekipmanları, Sistemleri ve Hizmetleri aracılığıyla oluşturulan, keşfedilen, kullanılan, erişilen, indirilen, depolanan, iletilen, alınan veya silinen yazılı Elektronik İletişimler ile ilgili olarak gizlilik beklentisi içinde olmamalıdır. Citi, Elektronik İletişim Ekipmanları, Sistemleri ve Hizmetleri ile Elektronik İletişimleri izleyebilir. Bu Elektronik İletişimlerin sahibi Citi'dir ve geçerli kayıt tutma gerekliliklerine uygun olarak elde tutulabilir (yerel yasa ve regülasyonlara tabi olarak).

<https://policydirectory.citi.net/cpd/layouts/15/DocIdRedir.aspx?ID=CPDPROD-13-8739>

11 SİYASİ FAALİYETLER VE KATKILAR

Aşağıdakilerle ilgili yasalar gibi çeşitli kanunlar: yabancı etkisi; kampanya finansmanı; hediyeler ve ağırlamalar; yasama, kamuoyu (taban), itibar ve düzenleyici kurum nezdindeki lobi faaliyetleri; tedarik, "ödeme karşılığı iş alma" (pay-to-play); ve menkul kıymetler konuları, Citi ve Tedarikçilerinin siyasi faaliyetlerini ve bu faaliyetlere ilişkin bildirimlerini düzenler. Tedarikçilerin ilgili Citi politikalarına veya standartlarına, yasalarına veya regülasyonlarına uymayan herhangi bir siyasi faaliyette bulunması yasaktır.

Siyasi faaliyet aşağıdakileri içerir ancak bunlarla sınırlı değildir:

1. Kurumsal veya kişisel siyasi katkılarda bulunma, siyasi katkıları isteme, şirket fonlarını veya kaynaklarını kullanma (ör., tesisler, ekipman, yazılım veya personel) ve bir siyasi makam, bir siyasi parti komitesi veya bir siyasi komite için kampanya yapan bir aday adına şirket zamanı esnasında kişisel hizmetler için gönüllü olma.
2. Memurları, mevzuatı etkileme girişimleri dâhil olmak üzere doğrudan veya üçüncü taraflar yoluyla lobicilik yapma ya da kamu görevlilerine ulaşma girişiminde bulunma, yargılama alanına bağlı olarak kurum kural koyma işlemini etkilemeye ve devlet sözleşmelerini vermeye yönelik girişimleri içerebilir; veya
3. Herhangi bir resmî kurul, komisyon veya diğer benzer organizasyon dâhil olmak üzere bir hükûmetle ilişkili herhangi bir siyasi makamı isteme, kabul etme veya elde tutma.

Citi'nin Hükûmetle İlişkiler Global Operasyon Kontrolünün (ggacontrol@citi.com) önceden yazılı izni olmaksızın Citi veya müşterileri adına (veya adınaymış gibi görünen) herhangi bir Tedarikçi tarafından hiçbir siyasi faaliyet üstlenilemez veya yürütülemez. Citi, Tedarikçi tarafından sunulan lobicilik gibi sözleşmeli ve izin verilebilir siyasi faaliyet hizmetleri için bir ücret ödeyebilir ve/veya cepten yapılan harcamaların ödemesini yapabilir, ancak Citi herhangi bir türde kişisel veya kurumsal siyasi katkı için asla bir Tedarikçiye veya çalışanlarından herhangi birine geri ödeme yapmayacaktır.

12 KARA PARA AKLAMA İLE MÜCADELE (“AML”)

Müşteriyle ilgili belirli hizmetleri (ör., işe kabul, müşteri hesabı ve işlem taraması) gerçekleştiren veya yukarıdaki faaliyetlerle ilgili veri/metrik sunan VE/VEYA finansal işlemler ya da araçlarla ilgili olarak aracılık yapan (ör., uzaktan çek yatırma, kurye, zırhlı araç veya Lockbox tahsilat hizmetleri, elektronik transferler, dijital varlıklar) Tedarikçiler için geçerlidir.

12.1 AML Yükümlülükleri:

1. Citi Süreçlerine ve Yürürlükteki Yasalara uygunluk:

- (i) Gramm-Leach-Bliley Act ve bu Kanun kapsamında çıkarılan regülasyonlar; (ii) USA PATRIOT Act ve bu Kanun kapsamında çıkarılan regülasyonlar; (iii) kara para aklamayı ele alan herhangi bir yasa veya regülasyon ve (iv) ekonomik yaptırımlarla ilgili herhangi bir yasa veya regülasyon dâhil olmak üzere yürürlükteki yasaların gerekliliklerini karşılamak üzere tasarlanan Citi süreçlerini ve prosedürlerini sürdürmek ve bunlara uymak. Bu tür politikalar ve prosedürler, finansal aktiviteler, işlemler ve nakit alımıyla ilgili olağan dışı veya potansiyel olarak olağan dışı görünen herhangi bir gözlemlenen aktivitenin derhâl raporlanması gereklilikleri de dâhil olmak üzere kara para aklamayı önleme rollerini ve sorumluluklarını ele alacaktır.

2. Personel için Yıllık Eğitim ve Program Unsurları:

- Citi'ye Hizmet sağlayan Personelinin, finansal aktiviteler, işlemler ve nakit alımıyla ilgili olağan dışı veya potansiyel olarak olağan dışı görünen herhangi bir aktiviteyi derhâl bildirme gereklilikleri de dâhil olmak üzere, kara para aklamayı önleme rolleri ve sorumlulukları konusunda yıllık eğitim almasını sağlamak. Eğitim, bunlarla sınırlı olmamak üzere, aşağıdaki bileşenleri kapsayacaktır:
 - a. Şüpheli aktivitelerin bildirilmesi ve eskale edilmesi.
 - b. Customer Identification Program (CIP), yaptırım ve ad taraması, müşteri durum tespiti (CDD), gelişmiş durum tespiti (EDD) ve **Nihai**

Faydalanıcıların (UBO'ların) belirlenmesi ve doğrulanmasını içeren bir "Know Your Customer" (KYC) programı.

- c. İlgili tüm finansal araçlar ve aktivitelerde işlem izleme.
- d. Yasal ve düzenleyici değişiklikler ile maddi AML programı değişikliklerine ilişkin raporlama dâhil olmak üzere periyodik raporlama/metrikler.
- e. saha ziyaretleri de dâhil olmak üzere AML programının etkinliğinin test edilmesi ve kontrol edilmesi

3. Sözleşme Hükümlerine Uyum:

- Tedarikçi tarafından uygulanması gereken herhangi bir programı tanımlayan herhangi bir Sözleşme hükmüne uyun.

4. Şüpheli İhlallerin Derhâl Bildirilmesi:

- Citi'yi veya müşterilerini ilgilendiren nakit alımı, finansal aktiviteler ya da işlemlerle ilgili olağan dışı veya potansiyel olarak olağan dışı görünen gözlemlenmiş herhangi bir aktivite dâhil olmak üzere, şüphelenilen yasa ihlallerini derhâl ve yazılı olarak Citi'ye bildirin.

5. Vergi Kaçakçılığının Önlenmesi ve Bildirilmesi:

- Faaliyet gösterdikleri ülkelerdeki tüm geçerli vergi kanunlarına ve regülasyonlarına uyun.
- Tedarikçiler hiçbir koşulda kasıtlı yasa dışı vergi kaçakçılığına girmemeli veya başkaları adına bu kaçakçılığı kolaylaştıramamalıdır; bunlar, vadesi gelmiş ve ödenecek vergilerin ödemesinden kaçınmaya veya vergi makamlarından bilgi gizlemeye yardımcı olacak aktivitelerde bulunmayı içerebilir.
- Bu bakımdan, Tedarikçiler vergi kaçakçılığı ile ilgili makul önleme prosedürlerini benimsemeli ve Citi ile ilgili herhangi bir ihlali veya şüpheli ihlali yazılı olarak derhâl Citi'ye bildirecektir.

12.2 Tedarikçi Kurum İçi Politika ve Prosedürleri:

Tedarikçiler, şu anda yürürlükte olan veya bundan sonra yürürlüğe girecek olan tüm AML yasa ve regülasyonlarına uyum sağlamak açısından uygun iç politika ve prosedürleri sürdürecektir.

13 KAYIT YÖNETİMİ

Citi Bilgilerine erişen/işleyen/depolayan Tedarikçiler için geçerlidir.

Citi, Citi Bilgilerini gözetiminde bulunduran tüm Tedarikçilerin, (i) Citi'nin kayıt yönetimi amaçları doğrultusunda Bilgileri Kayıt veya Geçici Bilgi olarak belirlemek ve sınıflandırmak, (ii) Kayıtları Citi Master Record Catalogue ("**MRC**") uyarınca sınıflandırmak, (iii) Bilgileri Citi'nin saklama gerekliliklerine göre saklamak ve (iv) herhangi bir Bilgi Bekletme bulunmaması hâlinde, Bilgi Yaşam Döngüsünün sonunda Bilgileri uygun şekilde imha etmek için Ticari Aktivite Sahibi ("**BAO**") veya birincil Citi iş irtibat kişisiyle birlikte çalışmasını şart koşar.

BAO veya birincil Citi iş irtibat kişisi, Tedarikçinin MRC'deki Citi kayıt kodlarına göre kayıtları tanımlayıp sınıflandırmasını ve Envanterin en az yılda bir kez güncellenmesini sağlamak için Tedarikçi ile birlikte çalışmalıdır. Tedarikçi, BAO tarafından bildirilen Kayıt Yönetimi gerekliliklerine uymakla yükümlüdür. İmha edilmeye ilişkin uygunluk kriterlerini karşılayan kayıtlar, mümkün olan en kısa sürede uygun şekilde imha edilmelidir, ancak bu süre, Bilgi Bekletme uygulamasına tabi olmadıkları sürece, saklama gereklilikleri karşılandıktan sonra altı aydan daha uzun olmamalıdır. Geçici Bilgiler, Bilgi Bekletme uygulamasına tabi olmadıkları sürece, son kullanımından itibaren iki yıldan fazla olmamak üzere imha edilmelidir. Kişisel bilgileri içeren Geçici Bilgiler, Bilgi Bekletmelerine tabi değilse, toplanma amacı karşılandıktan sonra silinmelidir. Tedarikçi, bir Bilgi Bekletmesi bildirildiğinde Citi Bilgilerinin imhasını veya değişikliğini askıya almalıdır. Tedarikçi, herhangi bir belirsizlik durumunda birincil Citi iş irtibat kişisine veya BAO'ya danışacaktır.

DRIM tarafından yapılan düzenleyici ve dâhilî değişikliklere uyum sağlamak amacıyla, Ülke Saklama Programlarında listelenen saklama kuralları üç ayda bir gözden geçirilir ve gerektiği şekilde güncellenir. Tedarikçiyi etkileyen bir değişiklik olması durumunda, BAO Tedarikçiye bilgi verecektir. Tedarikçi etkiyi değerlendirmeli ve ilgili sistemlerde, süreçlerde ve envanterlerde değişiklikler uygulamalıdır. BAO'dan gelen bildirimden itibaren 90 gün içinde sahip olduğu ve yönettiği Kayıt türleri.

Citi adına belgeleri muhafaza eden Tedarikçiler, BAO tarafından talep edildiği şekilde gerekli süre içerisinde yasal veya diğer bir yargılama ile ilgili olduğu düşünülen tüm Bilgileri korumaktan ("bekletmek"), toplamaktan ve üretmekten sorumludur. Tedarikçi, talep üzerine, geçerli sözleşme koşulları kapsamında gerekli olduğu şekilde Citi bilgilerini iade edecektir. Tedarikçiler, birincil Citi iş irtibat kişisinin veya BAO'nun onayı olmadan, sınıflandırmasına bakılmaksızın (örneğin Gizli, Gizli Olmayan) hiçbir Citi Bilgisini imha etmemelidir; bu onay, imha edilmesi gereken Bilgilere hiçbir aktif Bilgi Bekletme uygulanmadığının onayını içermelidir. Kayıt Yönetimi ve saklama gereklilikleri ve diğer tüm bilgi işleme gereklilikleri, aksi açıkça kararlaştırılmadığı takdirde, Sözleşmenin feshedilmesinden veya sona ermesinden sonra da geçerliliğini koruyacaktır.

Tedarikçiler, Tedarikçinin gözetimi altındaki Citi Bilgilerinin yönetimini denetlemekten sorumlu tüm Tedarikçi Personelinin listesini içeren belgeleri muhafaza edecek ve birincil Citi iş irtibat kişisi veya Kayıt Yönetim Görevlisi ile irtibat kişisi adlarını, prosedür ayrıntılarını, rolleri ve sorumlulukları ve Citi'nin Tedarikçi Kayıt Envanterini gözden geçirmek ve güncellemek için periyodik toplantılar yapacaktır.

14 KURUMSAL DİRENÇ/İŞ SÜREKLİLİĞİ

Citi tarafından kullanılan hizmetleri sağlayan veya teknoloji altyapısını/uygulamalarını barındıran Tedarikçiler için geçerlidir. Citi Ticari Aktivite Sahibi (BAO), uygulanabilirliği ve COB gerekliliklerini Tedarikçiye iletmekten sorumludur.

14.1 Kurtarma Kaynakları

Tedarikçilerin Felaketten Kurtarma Planı, Tedarikçinin birincil konumları devre dışı kaldığında Citi'ye tüm ürünleri ve hizmetleri teslim edebilecek alternatif kaynakları sağlamalıdır. Kurtarma kaynakları coğrafi olarak birincil kaynaklardan farklı konumlarda, aynı felaket olayının hem birincil hem de kurtarma konumlarını etkileyebilme tehdidini en aza indirecek veya ortadan kaldıracak kadar yeterli ayrıma sahip bir şekilde konumlandırılmalıdır.

1. Kurtarma kaynakları, Bilgi Sistemleriyle sınırlı değildir, ancak Citi'ye ürünlerin ve hizmetlerin devam eden teslimatı için gereken tüm kaynakları içerir ve personel, binalar, iş ekipmanı, veri merkezleri, veri ve ses ağları ve ulaştırma hizmetleri içerebilir.
2. Uygulama tedarikçileri, Yüksek Kullanılabilirlik (HA) yapılandırmasını sağlamak için Sıcak/Sıcak tipi bir mimari uygulayabilir. Bu mimari, istemcilerin/kullanıcıların kullanımına açık, çalışır durumda olan ve en az iki adet aynı şekilde yapılandırılmış sistemin olmasını gerektirir. Bu modelin sunduğu en önemli özellik, alternatif ortamların birincil (üretim) veri merkeziyle eş zamanlı olarak çalışıyor olmasıdır.

14.2 Kurtarma Hizmet Seviyeleri

Tedarikçinin iş devamlılığı, Citi için yürürlükte olması amacıyla yerleşik hizmet düzeylerini karşılamalıdır. En azından, Tedarikçinin Felaketten Kurtarma Planı aşağıdakiler için belirli değerleri belirleyecektir:

1. Kurtarma Süresi Hedefi
2. Kurtarma Noktası Hedefi
3. Kurtarma Kaynakları/Teknoloji Kapasitesi
4. Kurtarma Süresi

14.3 Felaketten Kurtarma Planı

Tedarikçi, Tedarikçinin Ürünleri/Hizmetleri sağlama veya işbu Sözleşme kapsamındaki diğer yükümlülüklerini belirli diğer bir konumdan veya belirli kişilerin çabaları aracılığıyla yerine getirme kabiliyetindeki herhangi bir kesintiye rağmen, Tedarikçinin Ürünleri/Hizmetleri derhâl sağlayabileceği ve yükümlülüklerini alternatif bir konumdan veya yedek Personel ile yerine getirebileceği bir şekilde, işin devamı için bir Felaketten Kurtarma Planı sürdürecektir (ve Citi tarafından talep edilmesi hâlinde mevcut ve

periyodik testlerinin kanıtını sağlayacaktır). Felaketten Kurtarma Planının bir kopyası, Citi ile Tedarikçi arasında imzalanan her İş Emrinin Yürürlük Tarihinden itibaren on (10) takvim günü içinde ve sonrasında her İş Emri geçerli olduğu süre boyunca yılda bir kez Citi'ye sunulmalıdır. Tedarikçi, Felaketten Kurtarma Planını başlattığı durumlarda Citi'nin Tedarikçiden Ürün/Hizmet almaya devam etmesi için gerekli tüm talimatları veya diğer bilgileri Citi'ye sağlayacaktır. Tedarikçi, Felaketten Kurtarma Planının asgari olarak şunları içereceğini beyan, garanti eder ve taahhüt eder:

1. Teknolojinin kullanılamaması (Hizmet Reddi/DoS), birincil çalışma konumunun kullanılamaması (Erişim Reddi/DoA) ve personelin (alt yükleniciler dâhil) kullanılamaması gibi kesintilerin etkilerini azaltmak amacıyla yer değiştirme, işin aktarılması ve/veya uzaktan erişim dâhil kurtarma prosedürleri ve stratejileri;
2. Tedarikçi tarafından Ürün/Hizmet konumlarından ayrı bir ikincil felaket kurtarma sitesinin bakımı (bunlarla sınırlı olmamak üzere), yedekleme medyasının Ürün/Hizmet konumlarından ayrı bir konumda depolanması, yedekli iletişim hatları ve sunucuların kullanımı;
3. Karşılıklı olarak kararlaştırılan bir süre içinde operasyonları yeniden başlatmaya yönelik süreç ve prosedürleri içeren; elektrik kesintisi, sistem arızası, doğal afet veya diğer öngörülemez koşullar nedeniyle Ürünlerde/Hizmetlerde yaşanan uzun süreli bir kesintiye müdahaleye ilişkin ayrıntılı ve belgelenmiş bir plan da dâhil olmak üzere, Ürünlerin/Hizmetlerin işletilmesi ve uygulanmasına yönelik yedekleme/geri yükleme prosedürleri;
4. Tüm İçeriğin korunmasına yönelik Prosedürler;
5. Değiştirme ekipmanı (ör., bilgisayar ekipmanı) için prosedürler ve herhangi bir üçüncü taraf anlaşmaları;
6. Herhangi bir saha dışı üretim tesisi için prosedürler; ve
7. Tedarikçinin Felaketten Kurtarma planı şunları sağlayacaktır:
 - a. Tedarikçi, Ürünleri/Hizmetleri olumsuz etkileyebilecek herhangi bir felaketi derhâl Citi'ye bildirecektir;
 - b. Tedarikçi, Citi'ye söz konusu bildirimden sonraki 24 saat içinde Ürünleri/Hizmetleri alternatif bir işleme tesisinde sunmaya devam etmek için bir plan sunacaktır;
 - c. Ürünler/Hizmetler, ilgili sözleşmede aksi belirtilmediği sürece, Citi tarafından kritiklik derecesi "İşletme Kritik" veya "YÜKSEK" olarak derecelendirilen süreçler için 4 saat veya daha az olan, Citi tarafından kritiklik derecesi "ORTA" olarak derecelendirilen süreçler için 24 saat veya daha az olan ve Citi tarafından kritiklik derecesi "DÜŞÜK" olarak derecelendirilen süreçler için 72 saat veya daha az olan gerekli Kurtarma Zamanı Hedefi (RTO) dâhilinde tam olarak çalışır durumda olmalıdır; ve
 - d. Tedarikçi tesislerinin bazı bölümleri çalışmaz durumdaysa, Tedarikçi Citi'ye, Tedarikçinin diğer ticari müşterilerine davrandığından daha az adil davranmayacaktır.

14.4 Barındırılan Hizmetler için Geçerli Felaketten Kurtarma Planı Gereklilikleri

Tedarikçinin Citi'ye Barındırılan Hizmeti yönetmesi ve sağlaması durumunda, aşağıdaki hükümler de geçerli olacaktır. Felaketten Kurtarma Planı en azından şunları içerecektir:

1. Karşılıklı olarak kararlaştırılan bir süre içinde operasyonları yeniden başlatmaya yönelik süreç ve prosedürleri içeren; elektrik kesintisi, sistem arızası, doğal afet veya diğer öngörülemeyen koşullar nedeniyle Hizmetlerde yaşanan uzun süreli bir kesintiye müdahaleye ilişkin ayrıntılı ve belgelenmiş bir plan da dâhil olmak üzere, Barındırılan Hizmetlerin işletilmesi ve uygulanmasına yönelik yedekleme/geri yükleme prosedürleri;
2. Ayrıca, Tedarikçinin Felaketten Kurtarma Planı şunları sağlayacaktır: (a) Tedarikçi, Barındırılan Hizmetleri olumsuz etkileyebilecek herhangi bir felaket durumunda Citi'yi iki (2) saat içinde yazılı olarak bilgilendirecektir; (b) Tedarikçi, Citi'ye bu bildirimden sonraki 24 saat içinde Barındırılan Hizmetleri alternatif bir işleme tesisinde sağlamaya devam etmek için bir plan sunacaktır ve (c) Barındırılan Hizmetler ilk bildirimden itibaren 48 saat içinde tam olarak çalışır duruma gelmelidir;
3. Tedarikçi, talep üzerine, Citi'nin Tedarikçinin Felaketten Kurtarma Planı ve iş sürekliliği planıyla uyum içinde çalışacak bir felaketten kurtarma planı ve iş sürekliliği planı geliştirmesine olanak tanımak için gerekli bilgileri sunmayı kabul eder; ve
4. Tedarikçi tesislerinin bazı bölümleri çalışmaz durumdaysa, Tedarikçi Citi'ye, Tedarikçinin diğer ticari müşterilerine davrandığından daha az adil davranmayacaktır.

14.5 Felaketten Kurtarma Planındaki Değişiklikler

Tedarikçi, Felaketten Kurtarma Planını, değişiklikler Felaketten Kurtarma Planını hizmetleri olumsuz yönde etkileyecek bir şekilde (örneğin, RTO'larını uzatmak) bozmadığı sürece değiştirebilir. Tedarikçi, Felaketten Kurtarma Planındaki değişiklikleri derhâl Citi'ye bildirecek ve Citi'nin talebi üzerine, Citi'nin değişiklikleri tam olarak anlayıp yanıtlayabilmesi için değişiklikleri açıklayacaktır.

14.6 Alt Yüklenicilerin Felaketten Kurtarma Planı

Tedarikçi, Tedarikçinin herhangi bir Alt Yüklenicisinin, Citi'nin Tedarikçilere Yönelik Gereklilikleri ile uyumlu bir Felaketten Kurtarma Planı ve ilgili İş Sürekliliği kontrolleri sürdürmesini sağlayacaktır. Tedarikçi, bu tür kontrollerin ve test sonuçlarının periyodik olarak incelenmesi ve tespit edilen boşlukların zamanında düzeltilmesini sağlamak dâhil olmak üzere Alt Yüklenicilerin uygun gözetimini sağlamalıdır.

14.7 Felaketten Kurtarma Planının Devreye Alınması ve Kriz Bildirimi

Tedarikçi, birincil Citi iş irtibat kişisine derhâl şunları bildirecektir:

1. Tedarikçi, Felaketten Kurtarma Planını başlattığında ve;
2. Citi'ye sağlanan Hizmet veya Ürünlere olumsuz etkisi olması makul şekilde ihtimal dâhilinde olan, Tedarikçi veya Tedarikçi Alt Yüklenicileri aleyhindeki herhangi bir kriz, tehdit, uyarı veya siber vaka ile ilgili olarak.

14.8 Test

Tedarikçinin tüm kurtarma kaynakları ve planları, üretim uygulamasının ardından 120 gün içinde (Citi tarafından Kurumsal Kritik olarak sınıflandırılan uygulamalar için 90 gün) test edilmeli ve en az yılda bir (her 12 ayda bir) test edilmelidir. Test, Tedarikçinin Citi'ye teslim edilen tüm ürünler ve hizmetler için kurtarma hizmeti düzeylerini karşılayabildiğini gösterecektir. Bu testler kapsamlı olmalı ve Citi'ye sağlanan Hizmetlerin tüm kapsamını içermelidir. Tedarikçiler, Citi'ye sağlanan ürünlerin/hizmetlerin kurtarılmasına yönelik testin duyurusunu en az 30 takvim günü önceden Citi'ye bildirmelidir. Citi, Citi tarafından kullanılan uygulamaların kurtarma ortamında işlevselliğini doğrulamak amacıyla Tedarikçinin kurtarma testine katılabilir veya bu testi gözlemleyebilir. Citi katılmak isterse Tedarikçi, testi gerçekleştirmeden önce Citi'ye test hedeflerini, test planını ve test alanına bağlanma prosedürlerini sağlayacaktır. Her testi tamamladıktan sonra on (10) iş günü içinde, Tedarikçi, geri kazanmak için gereken süreler ve test sonuçlarının kanıtı (ör., ekran görüntüleri) dâhil olmak üzere, test hedeflerinin bir özetini, test planını ve test sonuçlarını Citi'ye sunacaktır.

14.9 Hacim Doğrulaması

Citi tarafından Kurumsal Kritik olarak sınıflandırılan uygulamaları barındıran bir Tedarikçi, Üretim hacimlerinin COB / felaketten kurtarma ortamında işlenebileceğini göstermelidir. Citi ve Tedarikçi, doğrulama için kullanılacak olan metodoloji üzerinde anlaşmaya varmalıdır.

14.10 Hizmetlerin Sağlanması için Citi Sistemlerinin Kullanımı

Citi veya Citi'nin Bağlı Şirketleri tarafından talep edilmesi hâlinde, Citi Sistemlerini kullanan Tedarikçiler, Citi'nin felaketten kurtarma tatbikatlarına Citi'ye herhangi bir ücret veya ücret ödemedenden katılacaklardır.

14.11 Test Bulgularını Ele Alma

Tedarikçi'nin testindeki herhangi bir test sonucunun test hedeflerini veya ilgili RTO'yu karşılamaması durumunda, Tedarikçi kaynak neden analizi gerçekleştirmeyi ve tespit edilen eksikleri derhâl telafi edecektir. Söz konusu düzeltmenin uygulanmasının ardından Tedarikçi, ilk test başarısızlığından (veya ilgili İş Emrinde belirtilen süreden) itibaren en geç yüz yirmi (120) takvim günü içinde; Citi tarafından Kurumsal Kritik olarak sınıflandırılan uygulamalarda ise 90 takvim günü içinde yeniden test gerçekleştirecektir.

14.12 Kriz Yönetimi

İş devamlılık planı ile birlikte, Tedarikçi kurtarma operasyonlarının komuta ve kontrolü için bir kriz yönetim planını sürdürecektir. Tedarikçinin kriz yönetim planı en azından bir kurtarma operasyonunu başlatmak için yeterli yetkiye sahip belirli bireyleri tanımlayacak, kriz bilgilerinin toplanması ve dağıtılması için iletişim ve eskale etme protokollerini açıklayacak ve bir kriz durumunda Citi ile iletişime ilişkin bildirim ve eskalasyon protokollerini içerecektir.

14.13 İş Sürekliliği Değerlendirmeleri

Tedarikçiler; Tedarikçinin Citi gerekliliklerine ve iş sürekliliğiyle ilgili olarak Citi veya Tedarikçi için geçerli yasal ve/veya düzenleyici gerekliliklere uyumuna ilişkin politika,

prosedür ve kontrollerinin değerlendirilmesi amacıyla Citi Third-Party Continuity of Business Assessment Process'e tabidir. Değerlendirme, Tedarikçinin destekleyici kanıtlarla birlikte yanıt vermesini gerektiren anketlerden oluşur ve Tedarikçinin lokasyonlarına ziyaretleri içerebilir. Bir değerlendirmenin bulguları sorunları veya endişeleri ortaya çıkarır veya gösterirse, Citi bulguları belgeleyecek ve sorunları düzeltmenin bir yolunu belirlemek için Tedarikçiyle birlikte çalışacaktır. Tedarikçiler, Citi'nin kaygılarını Citi'yi makul düzeyde tatmin edecek şekilde ele almak için gerekli düzeltmeleri hızla yapmalı ve/veya telafi edici kontroller eklemelidir.

14.14 Operasyonel Direnç

Kritik Ticari Hizmetler, teslimatın kesintiye uğraması durumunda Citi'ye, müşterilerine veya finansal sisteme ciddi olumsuz etki yaratabilecek hizmetlerdir. Tedarikçi, Citi tarafından zaman zaman belirtildiği üzere, kritik iş hizmeti niteliğindeki veya Citi'nin kritik iş hizmetleri sunmasını destekleyen hizmet unsurlarının ("Kritik İş Hizmetleri") sunumundaki herhangi bir kesintinin, Citi tarafından belirlenen süreyi aşmamasını veya Citi tarafından belirlenip zaman zaman Tedarikçiye bildirilen ilgili herhangi bir metriği ("Etki Toleransları") ihlal etmemesini sağlayacaktır. Etki Toleransları, hizmet sunumunun kesintiye uğrayabileceği süreye eşit olan net bir zaman kısıtlı ölçüm olarak ifade edilecektir. Citi ve Tedarikçi, devam eden sözleşme yönetim sürecinin bir parçası olarak Etki Toleranslarını yıllık olarak gözden geçirecektir. Birden fazla Düzenleyici Kurumun gereklilikleri nedeniyle Citi'nin ayrı bir Kritik Ticari Hizmet için birden fazla Etki Toleransı belirlemesi gerektiğinde, Citi bu tür Kritik Ticari Hizmet için ayrı Etki Toleransı belirleyebilir. Tedarikçi:

1. Herhangi bir hizmeti Citi tarafından belirlenen ilgili Etki Toleransları dâhilinde sunmadığını (veya sunamamasının makul ölçüde muhtemel olduğunu) fark eder etmez, olası veya fiilî başarısızlığın nedenlerine ve başarısızlığın etkisini azaltmak için atılan adımlara ilişkin açıklamayla birlikte Citi'yi bilgilendirecektir;
2. Talep edildiğinde, Kritik İş Hizmetlerini destekleyen hizmeti Tedarikçinin sunabilmesi için gerekli kişileri, süreçleri, teknolojileri, tesisleri ve bilgileri Citi'nin belirlemesine olanak tanımak üzere Citi'ye makul yardım sağlayacaktır;
3. Citi'nin aşağıdakileri yapabilmesini sağlamak için Citi'ye makul yardım sağlayın:
 - a. Citi'nin veya Tedarikçinin operasyonlarında ciddi ancak makul olarak gerçekleşebilir bir kesinti olması durumunda, Tedarikçinin her bir Kritik İş Hizmeti için Etki Toleransları dâhilinde kalma becerisine ilişkin her türlü dâhilî senaryo testi; ve
 - b. Citi'nin zayıflıkları belirlemesini sağlamak için bir senaryo testinin ardından alınan dersler ve Tedarikçinin etkili bir şekilde yanıt verme ve gelecekteki aksaklıklardan kurtulma yeteneğini geliştirmek için gerekli tüm eylemler.

Citi tarafından yapılan herhangi bir dâhilî senaryo testi sonucunda, Tedarikçinin Citi tarafından belirlenen ilgili Etki Toleransları dâhilinde hizmetleri sunma becerisine ilişkin güvenlik açıkları veya sınırlamalar belirlediğinde ve Tedarikçinin Citi tarafından belirlenen ilgili Etki Toleransları dâhilinde hizmetleri sunamamasının ardından, taraflar,

Tedarikçinin bu tür güvenlik açıklarını veya sınırlamaları çözmek ya da azaltmak veya makul olarak uygulanabilir olduğu en kısa süre içinde Etki Toleransları (uygun olduğu şekilde) dâhilinde kalmak için kusurun nedenini düzeltmek için gerekli adımları atmasını sağlamak üzere bir plan (planı uygulamak için bir zaman çizelgesi dâhil) kararlaştıracaklardır.

14.15 Emanet Düzenlemesi

Citi'nin talebi üzerine, (i) Citi ortamında çalıştırılmak üzere Citi'ye yazılım lisanslayan veya (ii) Citi'ye Barındırılan Hizmet sağlayan Tedarikçiler, Mevduat Materyallerinin Citi'nin belirlediği emanet saklama acentesine teslim edilmesini sağlayacak ve geçerli emanet saklama sözleşmesi kapsamında Mevduat Materyalleriyle ilgili olarak acentenin talep ettiği mevduat sahibi kayıt çizelgesini veya diğer formları imzalayacak/dolduracaktır. Bundan sonra, lisans veya Barındırılan Hizmet ile ilgili geçerli sözleşmenin geri kalan süresi boyunca Tedarikçi, Citi tarafından kullanılan yazılım veya Barındırılan Hizmet sürümüne uygun en son yazılım sürümüyle emanet edilen Kaynak Kodunun ve diğer Mevduat Materyallerinin güncel kalmasını sağlamak için Mevduat Materyallerinin güncellenmiş sürümlerini emanet acentesine yatıracaktır. Kaynak Kodu veya diğer Mevduat Materyali güncellemeleri, Citi'ye lisanslı yazılımdaki herhangi bir güncellenmenin veya Citi tarafından kullanılan Barındırılan Hizmetlerdeki değişikliklerin tarihinden itibaren otuz (30) gün içinde emanetçiye teslim edilecektir. Tedarikçi, emanet sözleşmesinde belirtilen tüm yükümlülüklerle ve mevduat sahibinin gerekliliklerine tam olarak uyacaktır. Tedarikçi, kurulum ücretleri, yıllık ücretler, depozito ücretleri, hizmet ücretleri ve diğer tüm emanet ücretleri ve masrafları dâhil ancak bunlarla sınırlı olmamak üzere tüm emanet masrafları ve ücretlerinden tek başına sorumludur. Bir Serbest Bırakma Olayı durumunda, Emanetçi Temsilci, temel sözleşmenin ve emanet sözleşmesinin şartlarına uygun olarak, Mevduat Materyallerini Citi'ye veya Citi'nin görevlendirdiği kişiye serbest bırakacaktır.

Kaynak Kodu (veya diğer Mevduat Materyalleri) Citi'ye veya Citi'nin görevlendirdiği kişiye (doğrudan Tedarikçi tarafından veya geçerli bir emanet sözleşmesi kapsamındaki yükümlülüklerini yerine getirmek üzere Emanet Temsilcisi tarafından) teslim edilirse, Kaynak Kodu ve Mevduat Materyalleri, Tedarikçi ile Citi arasındaki ilgili sözleşme kapsamındaki mevcut lisansa tabidir; ancak her bir lisansın Citi'ye Kaynak Kodu ve diğer Mevduat Materyallerini makul ölçüde gerekli olduğu takdirde kullanma ve değiştirme hakkı verdiği kabul edilir: (i) Yazılımı ve diğer Mevduat Materyallerini Citi'nin Sistemleri ile bütünleştirmek ve uyumluluğunu sağlamak, (ii) Yazılımın veya diğer Mevduat Materyallerinin Uygulanabilir Kanun, endüstri standartları veya piyasa uygulamaları ile uyumlu olmasını sağlamak, (iii) Yazılımın veya diğer Mevduat Materyallerinin teknolojik yeniliklerle güncel kalmasını sağlamak ve (iv) Yazılımın ve diğer Mevduat Materyallerinin Citi'nin ve Bağlı Kuruluşlarının mevcut Lisans kapsamındaki ticari amaçlarını yerine getirmesini sağlamak. Kaynak Kodunu kullanarak Citi tarafından veya Citi adına geliştirilen bir değişikliği içeren Yazılımın herhangi bir sürümü, bu Bölümün ve temel sözleşmenin tüm hükümlerine tabidir; ancak Tedarikçinin herhangi bir değişiklik üzerinde hiçbir hakkı, mülkiyeti veya çıkarı olmayacak ve herhangi bir değişiklik üzerindeki tüm fikrî mülkiyet hakları münhasıran Citi'ye ait olacaktır.

Tedarikçi, Yazılımda kullanılan herhangi bir yazılımı sağlayan üçüncü taraflarla birlikte, Tedarikçinin söz konusu üçüncü taraf yazılımının kaynak kodunu Kaynak Kodu Deposuna yerleştirmesine olanak sağlamak için ticari olarak makul çabayı gösterecektir.

Üçüncü taraf Tedarikçiye bu hakkı vermeyi reddederse, Tedarikçi, bir Serbest Bırakma Olayı üzerine geçerli üçüncü taraf yazılım lisans sözleşmesinin Citi'ye devredilebilmesi için ticari olarak makul çabayı gösterecektir.

Bu Bölüm uyarınca Citi'ye teslim edilen Kaynak Kodu, Citi'nin iş ve operasyonel gereklilikleriyle bağlantılı olarak Kaynak Kodunu ve Yazılımı kullanması ve değiştirmesi, Yazılımın teknolojik yeniliklerle güncel kalmasını ve Uygulanabilir Yasalara uymasını sağlaması *koşuluyla*, geçerli lisanslı Yazılım veya Barındırılan Hizmetler için mevcut Lisansa tabi olacaktır. Kaynak Kodunu kullanarak Citi tarafından veya Citi adına geliştirilen bir değişikliği içeren Yazılımın herhangi bir sürümü, geçerli sözleşmenin tüm hükümlerine tabidir; ancak Tedarikçinin herhangi bir değişiklik üzerinde hiçbir hakkı, unvanı veya çıkarı olmayacak ve herhangi bir değişiklik üzerindeki tüm Fikrî Mülkiyet Hakları münhasıran Citi'ye ait olacaktır.

15 GLOBAL ARKA PLAN TARAMASI STANDARTLARI

Citi'ye hizmet sağlayan tüm Üçüncü Taraf Tedarikçiler için geçerlidir.

15.1 Genel Bakış – Arka Plan Taraması

Arka plan taraması yürürlükteki tüm yerel yasalara ve regülasyonlara uygun olarak yapılmalıdır. Bu belgede açıklanan tüm bilgi ve kişisel açıklamalar, uygun şekilde Tedarikçinin temsilcileri, Tedarikçinin personeli ve Alt Yüklenicileri tarafından sağlanmalıdır. Bir özgeçmiş, mülakat sırasında, işe kabul formunda veya işe kabul sürecinde bilgilerin tahrif edilmesi ya da atlanması, ne zaman tespit edilirse edilsin, yerel yasalar uyarınca Citi'de görevlendirmenin reddedilmesine veya sona erdirilmesine gerekçe oluşturabilir. Yapılan herhangi bir taramaya yönelik olumsuz sonuçlar, ne zaman ortaya çıkarsa çıksın, yerel kanun doğrultusunda Citi ile görevlendirmenin reddine veya feshine ilişkin gerekçeleri teşkil edebilir.

Arka plan taramasının tamamlanmasına ilişkin ek bilgiler https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf adresinde bulunabilir.

15.2 Temel Bilgilerin Toplanması ve Kimlik Doğrulaması

Herhangi bir Tedarikçi personeli Citi'deki görevlendirmesine başlamadan önce Tedarikçiler; ilgili kişinin adını, soyadını, posta adresini, farklıysa daimi adresini, telefon numarasını ve varsa e-posta adresini almalıdır. Tedarikçi Personeli ayrıca kimliğini doğrulayan dokümanları da sağlamalıdır. Bu, bir ulusal kimlik numarasının, devlet tarafından verilen resimli bir kimlik kartının veya pasaportun belgesinin ve/veya bilgilerinin sağlanmasını içerebilir.

15.3 Yaptırımlar Taraması

Citi adına iş yapan tüm Tedarikçi personeli veya Alt Yükleniciler dâhil bir Citi Tedarikçisinde %25 ya da daha fazla pay sahibi olan kişiler, Citi verilerine/sistemlerine/ağlarına VE/VEYA Citi tesislerine erişimleri olup olmadığına bakılmaksızın; United States Department of the Treasury's Office of Foreign Assets Control ("OFAC"), Specially Designated Nationals and Blocked Persons ("SDN") list ve

Amerika Birleşik Devletleri yaptırımlarına tabi bölge ve yargılama alanları listesine ("U.S. Sanctions") karşı ve ayrıca European Union (EU) Consolidated Financial Sanctions List, United Nations ("UN") Security Council Consolidated List, United Kingdom ("UK") Sanctions List ve yerel yargılama alanında geçerli yasa ve regülasyonlar uyarınca oluşturulan listeler ("Non-U.S. Sanctions") dâhil olmak üzere Amerika Birleşik Devletleri dışındaki yetkili makamların yayımladığı tüm listeler ve yaptırıma tabi yargılama alanlarının adlarıyla karşılaştırılarak taranmalıdır.

OFAC listeleri bu web sitesinde herkese açıktır: <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 Göçmenlik Uyumu

Tedarikçi, tüm personelin görevlendirme ülkelerinde çalışmak için yetkili olduğunu doğrulamak için protokoller sürdürdüğünü ve uyguladığını göstermelidir. Ek olarak, Tedarikçi: (1) tüm personelin çalışma iznine sahip olmasını sağlamak ve (2) çalışma uygunluğu ve doğrulama gereklilikleri dâhil olmak üzere yürürlükteki tüm yasa, regülasyon ve politikalara uyumu sürdürmek. Ayrıca, Tedarikçi personelinin sair suretle tüm geçerli göçmenlik kanunları ve regülasyonları ile uyumlu olmasını ve personelinin giriştikleri görevlendirmeler ve aktivitelere ilişkin vize için uygun statüye/sınıflandırmaya sahip olmalarını sağlamaya yönelik protokollere sahip olduğunu da göstermeli ve bunları sürdürmelidir.

15.5 İstihdam Geçmişi

Tedarikçiler, yerel regülasyona göre gerekirse son yedi (7) yıl veya 10 yıl boyunca personelinin istihdam geçmişini doğrulamalıdır. Bireyin iş geçmişi, işverenlerin, pozisyonların, tarihlerin ve görevlerin doğru bir şekilde temsil edildiğinden emin olmak için doğrulanmalıdır. Tedarikçinin personeli ayrıca Citi veya onun önceki şirketlerinden herhangi birinde danışman veya geçici işçi olarak daha önce çalışmış veya görevlendirilmiş olup olmadığını da açıklamalıdır (bunlarla sınırlı olmamak üzere: Citibank, Citicorp, Travellers, Salomon Brothers ve/veya Smith Barney).

15.6 Eğitim Geçmişi

Tedarikçiler, personelinin tamamlanan en yüksek eğitim seviyesini doğrulamalıdır. Doğrulanmış bilgiler, katıldığı tarihleri, kurum adlarını, adreslerini ve elde edilen dereceleri içermelidir.

15.7 Adli Sicil

Yasaların izin verdiği durumlarda Tedarikçilerin personeli ve alt yüklenicileri; suçu kabul veya itiraz etmeme beyanı ve yargılama öncesi yönlendirme ya da benzer bir programa katılım dâhil olmak üzere herhangi bir cezai suç nedeniyle tutuklama, çağrı, mahkeme celbi, hâkim karşısına çıkarılma, iddianameyle suçlanma veya mahkûmiyete tabi olmaları hâlinde bunu Citi'ye açıklamalıdır. Adli sicil kayıtları ve/veya parmak izi kontrollerine ilişkin idari inceleme, yasaların izin verdiği ve bunun mümkün olduğu durumlarda görevlendirmenin başlangıç tarihinden önce tamamlanmalıdır. Hırsızlık, dolandırıcılık, sahtekârlık veya güven ihlali ile ilgili suçlardan veya yerel yasalarca farklı şekilde

tanımlanan benzer suçlardan kaynaklanan cezai mahkumiyetler, aksi yasalarca yasaklanmadığı sürece Citi'ye atanmanın reddedilmesi ve/veya uygunsuz hâle getirilmesiyle sonuçlanabilir. Diğer cezai mahkûmiyetler geçerli yerel kanunlara ve regülasyonlara dayalı olarak görevlendirmenin reddi ve/veya mahrumiyeti ile sonuçlanabilir.

15.8 Yeniden Tarama

Görevlendirmesi sona eren Tedarikçi Personeli, Citi'ye yeniden atanmaları durumunda yeniden taranmalıdır. Yeniden tarama gereklilikleri hakkında ek bilgi için lütfen şu adrese bakın:

https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf

15.9 Uluslararası Transferler

Tüm taramalar, görevlendirmenin yapıldığı ülkenin regülasyonları doğrultusunda tamamlanmalıdır. Tedarikçi personeli yeni bir ülkeye transfer olursa, birey yeni ülkenin gerekliliklerine göre yeniden taranmalıdır.

16 GİDERLER

Sözleşmeye bağlı olarak geri ödenebilir işletme masrafları talep etmeye uygun Tedarikçiler.

16.1 Genel Bakış

Citi yalnızca, ürün ve hizmetlerin Citi'ye tedariki ile bağlantılı olarak Citi tarafından önceden yazılı şekilde onaylanmış olan ve Tedarikçi tarafından yapılmış olan, uygun durumlarda, geçerli Sözleşmenin şartlarına veya Citi'nin İşletme Masraf Yönetimi Politikasına ve ilgili Standartları ve Prosedürlerine uygun olan ve destekleyici makbuzlar, faturalar, seyahat programları veya Citi tarafından kabul edilen diğer belge türleri ile doğruluğu yeterli şekilde kanıtlanan işle ilgili makul giderlerin geri ödemesini yapacaktır.

16.2 Geri Ödemeler

Bu giderler, Citi faturalandırma gereklilikleri doğrultusunda uygun biçimde belgelendirilmeli ve Citi'ye faturalandırılmalıdır. Tedarikçi masrafları bir Citi çalışanı tarafından bir Tedarikçi adına karşılanmamalıdır. Geçerli ve onaylanmış bir gider kaleminin geri ödenmesi için Citi'ye sunulan herhangi bir gider (diğer tüm faturalama gerekliliklerine ek olarak) şunları içermelidir:

1. Giderin ticari amacı;
2. Giderin tutarı ve açıklaması;
3. Giderin yeri ve tarihi;
4. Tedarikçinin hizmet sağladığı projenin adı/tanımı;
5. Bu tür masrafların yapıldığı hizmetleri talep eden Citi temsilcisinin adı ve ticari ilişkisi; ve
6. Uygun olduğu durumlarda Satın Alma Siparişi numarası.

İzin verilen geri ödenebilir iş giderleri hakkında bilgi için lütfen birincil Citi iş irtibat kişinizle iletişime geçin. Destekleyici makbuzlar, faturalar, seyahat programları veya Citi tarafından kabul edilebilir olarak görülen diğer türden belgeler geri ödeme talebiyle birlikte gönderilmelidir. Geri ödeme talepleri, ilgili Sözleşmedeki hükümlerle veya, uygun olduğu durumda, Citi'nin İşletme Masraf Yönetimi Politikasıyla ve ilgili Standartları ve Prosedürleriyle uyumlu olmalıdır ve uygun iş sponsoru ve/veya birincil Citi iş irtibatı tarafından onaylanmalı ve uygun şekilde yetkilendirilmiş olan ve ilgili emtiaya ilişkin olarak yeterli bir tutara sahip olmalıdır. Uygun olmayan talepler geri ödenmeyecektir.

17 BİLGİ GÜVENLİĞİ (IS)

Ekte sınıflandırıldığı ve tanımlandığı şekilde herhangi bir Citi Bilgisine erişen, işleyen, saklayan veya yöneten; veya Citi markalı İnternet'e yönelik uygulamaları barındıran; veya Citi'nin ağ kaynaklarına bağlantısı olan; veya Citi tesislerine refakatsiz erişim gerektiren Alt Yükleniciler dâhil Tedarikçiler için geçerlidir.

17.1 Genel Bakış

Bu Bölüm, Citi Bilgilerini saklayan, işleyen, yöneten veya bunlara erişen veya Citi uygulamalarını barındıran veya Citi'ye ağ bağlantısı olan satıcı alt işleyicileri veya alt yüklenicileri de dâhil olmak üzere Citi Tedarikçileri için, Citi tarafından beklenen bilgi koruma kontrolleriyle ilgili asgari gereklilikleri sağlar. Bu gereklilikler, Citi ve Tedarikçilerinin iş yaptığı yerlerde bilgilerin geçerli yasal ve düzenleyici gerekliliklere ve en yüksek endüstri standartlarına (ör. ISO/IEC 27001/2) uygun olarak korunmasını sağlar. Yerel kanunlar, regülasyonlar veya ilgili endüstri standartları burada verilenlerden daha yüksek bir standardı teşkil ediyorsa, Tedarikçiler bu kanunlara, regülasyonlara veya standartlara uymalıdır. Ek olarak, Tedarikçilerin ek bilgi güvenliği uygulamalarını ve prosedürlerini, uyumlarının bir parçası olarak diğer Citi politikalarına ve sözleşmeye bağlı koşul ve şartlara dâhil etmeleri zorunlu olabilir. Tedarikçi, bilgi güvenliği için ek güvenlik uygulamaları veya prosedürler uygulamaya karar verirse, Tedarikçi bu uygulamaların ve prosedürlerin bu bölümde tanımlanan minimum kontrollerle çalışmamasını sağlamalıdır.

17.2 Bilgi Güvenliği Politikası ve Yönetişim

Tedarikçiler belgelenmiş bilgi güvenliği politikalarına ve standartlarına sahip olmalıdır. Politika yönetimi, açıkça tanımlanmış rolleri ve sorumlulukları ve teknolojinin mevcut durumu, endüstri standartları, yasal ve düzenleyici gereklilikler ile tutarlılık için yıllık politika ve standart incelemesini/güncellemesini içermelidir.

17.3 Görevlerin Ayrımı

Tedarikçiler, riski hafifletmek için yeterli telafi edici kontroller olmadığı müddetçe, hiçbir münferit kişinin yetkilendirme veya tespit olmaksızın aynı aktivite, değişim, Bilgi Sistemi veya işlem için sürekli erişimle herhangi iki iş fonksiyonunu veya iki Bilgi İşlem fonksiyonunu ya da iki Kontrollü Bilgi Sistemi fonksiyonunu gerçekleştirememesini sağlayan süreçlere sahip olmalıdır.

Tablo A

Fonksiyonlar	Fonksiyon Tanımı
Geliştirme/Mühendislik	Yazılım, donanım ve konfigürasyonları tasarlama, oluşturma veya değiştirme; örnekler şunları içerebilir: - Yeni uygulama kodu ve ilgili veri tabanı şemalarını tasarlama ve oluşturma - Altyapı ürünleri ve uygulama bileşenlerinin mühendisliğini yürütme - Teknolojik ürünleri yazılım ve hizmetlerle entegre olacak şekilde özelleştirme
Onaylama	Uygulamaya alınacak kod değişikliklerinin yayına alınmasını onaylama
Sistemleri Uygulama/Yönetme	Yazılım, donanım ve konfigürasyon değişikliklerini kurma, dağıtma veya yönetme. Örnekler şunları içerebilir: - Canlı altyapıya otomatik veya manuel kod sürümü gerçekleştirme - Bir teknoloji ürününün veya cihazının kurulumunu yapma - Canlı veriye sahip sistemlerde sorun giderme ve düzeltme süreçlerini desteklemek amacıyla servisleri başlatma veya durdurma
Ayrıcalıklı Kimlik Eylemlerini İnceleme	Değişiklik yönetimi faaliyetlerini veya güvenlikle ilgili sistem olaylarını doğrulama (ör. denetim izleri)
Kimlik Yönetimi	Kimlikleri (Kullanıcı, FID'ler ve Botlar), yetkileri veya parolaları ekleme, değiştirme ve silme
İş Fonksiyonu	Fonksiyon Tanımı
Ticari İşlem Başlatma	Ticari işlemleri başlatma (giriş yapma, yapma veya oluşturma olarak da adlandırılır) ve müşteri bilgilerini değiştirme
Ticari İşlemi Onaylama	Ticari işlemleri onaylama (yetkilendirme, kontrol etme veya serbest bırakma olarak da adlandırılır)
BT Fonksiyonu	Fonksiyon Tanımı
Ağ Operasyonları	Ağ altyapısı hizmetleri sağlayan ürünlerin cihaz yönetimini ve operasyonel desteğini yürütme. Ağ yönlendiricileri anahtarlar, güvenlik duvarları ve Alan Adı Hizmetleri (DNS) bunlara örnektir
Ağ Dışı Operasyonlar	Ağ altyapısı hizmeti sağlamayan ürünlerin cihaz yönetimini ve operasyonel

	desteğini yürütme. Sunucular, telefonlar ve bilgisayarlar bunlara örnektir
--	--

17.4 Yönetimin Bilgi Güvenliği Taahhüdü

Citi markalı, internete dönük bir uygulama barındıracak ve/veya Gizli ya da daha yüksek sınıflandırılmış Citi Bilgilerine erişecek Tedarikçiler; Tedarikçinin Citi gerekliliklerine ve bilgi güvenliğiyle ilgili olarak Citi veya Tedarikçi için geçerli yasal ve/veya düzenleyici gerekliliklere uyumuna ilişkin politika, prosedür ve kontrollerinin değerlendirilmesi amacıyla Citi Third-Party Information Security Assessment Process'e (TPISA) tabidir.

Değerlendirme, Tedarikçinin destekleyici kanıtlarla birlikte yanıt vermesini gerektiren güvenlik anketlerinden oluşur ve Citi'nin Gizli veya daha yüksek gizlilik dereceli Bilgilerinin saklandığı, işlendiği, yönetildiği veya üçüncü taraflarca erişildiği Tedarikçi lokasyonlarına ziyaretleri içerebilir. Ek olarak, TPISA Üçüncü Taraf Sürekli İzleme Ekibi, kullanım ömrü sona ermiş yazılımlar, istismar edilen açık bağlantı noktaları, güvenlik açıkları veya diğer tehlikeler gibi savunmasız İnternet sistemlerini, ana bilgisayarları, uygulamaları ve sunucuları belirlemek için kamuya açık bilgileri kullanan Siber Güvenlik izleme araçlarını kullanarak Tedarikçiyi izleyebilir. Muhtemel TPISA bulguları, güvenlik açıklarını belirtir veya işaret ederse, Citi, bulguları Tedarikçiye gönderilecek bir bildirimde belgelendirecek ve kusurların düzeltilmesine ilişkin yolları belirlemek üzere Tedarikçi ile çalışacaktır. Tedarikçiler, Citi'nin kendi takdirine bağlı olarak, sorunlar Citi tarafından risk derecesine tabi olduğundan, Citi'nin endişelerini gidermek için gerekli düzeltmeleri, eklemeleri/veya telafi edici kontrolleri hızla yapmalı ve Yüksek Riskli sorunlar için 180 takvim günü, Orta Riskli sorunlar için 240 takvim günü ve Düşük Riskli sorunlar için bir sonraki uyumluluk tarihinden önce gerekli zaman çizelgelerini karşılamalıdır.

1. Tedarikçi, kendi bilgi güvenliği standartlarına, politikalarına ve prosedürlerine karşı düzenli olarak iş operasyonlarının değerlendirmelerini ve ilgili kontrolleri yapmalıdır. Periyodik değerlendirmeler en azından aşağıdakileri içermelidir:
 - a) Tedarikçinin kendi Bilgi Güvenliği (IS) politikası ve standartlarına uyumu sağlamak için kullandığı süreçlerin değerlendirmesi.
 - b) Destekleyici kaynakların değerlendirmesi; örneğin, Tedarikçi tarafından kullanılan uygulamalar ve altyapı ve iş operasyonlarını destekleyen veya Citi'nin bu tür değerlendirmeler yapmasına izin vermek için Tedarikçinin alt yüklenicileri tarafından kullanılan IS süreçleri gibi. Üçüncü bir tarafın, Citi tarafından Gizli veya daha yüksek olarak sınıflandırılan Citi Bilgilerine erişen, bu bilgileri işleyen, yöneten veya ortadan kaldıran bir alt yüklenici ile yeni bir sözleşme yapması veya mevcut bir sözleşmeyi yenilemesi durumunda uyum gerekir.
2. Herhangi bir Bilgi Güvenliği Risk Değerlendirmesinin (ör. TPISA) bir sonucu olarak tanımlanmış olan sorunları belgelendirilmeli ve Citi'ye sağlanan iyileştirme kanıtlarıyla birlikte sorunlar kapanana kadar izlenmelidir.
3. Tedarikçinin Bilgi Güvenliği yönetim fonksiyonu ülke sınırları genelinde yer değiştirmişse, söz konusu yer değiştirme öncesinde Tedarikçi Citi'nin belgelendirilmiş onayını almalıdır.
4. Tedarikçi yeni bir tüzel kişiliği satın alırsa, Tedarikçi bu Standartlara uyum için satın alınan tüzel kişiliğin bir değerlendirmesini tamamlamalıdır.

5. Tedarikçi, Citi Bilgilerini saklamak, işlemek ve/veya iletmek için kullanılan sistemlere ilişkin güvenlik duvarı yönetimi, güvenlik yapılandırması yönetimi, yama yönetimi veya Bilgi Güvenliği İdaresi (ISA) işlevleri dâhil ancak bunlarla sınırlı olmamak üzere güvenlik yönetimi işlevlerini, Citi önceden yazılı olarak onaylamadıkça dış kaynak kullanımına devretmemelidir.
6. Tedarikçi, Citi Bilgileri içeren veya Citi markalı bir yazılım ya da web sitesi barındırıyorsa Citi'nin System Security Testing Standard (SSTS) belgesine uygun olarak periyodik güvenlik açığı değerlendirmeleri yapılmalı ve değerlendirme sırasında belirlenen önemli sorunlar söz konusu Standard'da belirtilen süreler içinde giderilmelidir. SSTS haricî dağıtım için onaylanmadığından Tedarikçiler, referans belgelere uygunluğu sağlamak için Citi İlişkiler Yöneticileri ile birlikte çalışmalıdır. Ayrıca, Tedarikçi, ilgili ISO/IEC 27001 Bilgi Güvenliği yönetim standartlarına (veya daha yüksek standartlar ve protokoller oluşturan halef bilgi güvenliği yönetim standartlarına) uyacaktır ve bu Bölüm 17'de yer alan bilgi güvenliği hükümlerine uymalıdır.
7. Citi kurum içi ağında sunuculara ve/veya Bilgi Sistemlerine bağlanmak gerekirse, Tedarikçi mevcut bağlanma tedarik sürecinin izlenebilmesi için kendi birincil Citi iş irtibatını bilgilendirmek zorundadır.
8. Tedarikçi, uygun Citi irtibatını [Ticari Aktivite Sahibi (BAO)] Citi Bilgilerinin yetkisiz erişimi veya edinimi ya da kaybı veya bozulması ya da silinmesi veya Citi Bilgilerini saklamak, işlemek almak veya iletmek için kullanılan Bilgi Sistemlerine yönelik diğer bir risk hakkında derhâl bilgilendirmelidir.
9. Tedarikçi, hassas verilerdeki tüm yüksek riskli aktivitelerin veya değişikliklerin, bu eylemleri gerçekleştiren kişilere atfedilmesini sağlayan denetim izlerine sahip olmasını sağlamalıdır.
10. Tedarikçi gizli veya daha yüksek gizlilik seviyesindeki verilerin ekran veya kâğıt üzerinde maskelendiğinden emin olmalıdır (örneğin, izleme, istisnai ve düzenleyici, ve diğer raporlar, vb. dâhil olmak üzere).
11. Tedarikçi 'kendi cihazları' ile yapılanlar dâhil olmak üzere hassas verilen yazdırılması, kaydedilmesi veya kopyalanmasını kısıtlamalıdır. Tedarikçi, yasa veya regülasyon aksini yasaklamadıkça, Sözleşme süresi içinde kararlaştırılan bir zamanda veya Sözleşmenin sonunda tüm Citi Bilgilerini iade etmeli ya da imha etmelidir.
12. Tedarikçi, Citi bilgilerine erişime sahip olan tüm Tedarikçi personelinin (çalışanlar, yükleniciler, geçici çalışanlar, alt yükleniciler) bir ifşa etmeme veya gizlilik anlaşması imzalamasını sağlamalıdır.
13. Tedarikçinin çalışanlarına, Tedarikçinin davranış kurallarının ve insan kaynakları politikalarının ihlal edilmesinden kaynaklanan uyumsuzluklara ilişkin disiplin sürecini içeren bir çalışan el kitabı veya benzer bir belge verilmeli ve çalışanlar bu belgeyi işe kabul süreçlerinin bir parçası olarak kabul etmelidir.
14. Tedarikçi, bir çalışanın veya çalışan olmayanın işine son verilmesi veya istifa etmesi durumunda tüm varlıkları almaya yönelik bir sürece sahiptir.
15. Herhangi bir Gizli Bilginin muhafaza edilmesi veya herhangi bir şekilde bir web sitesinde ya da web erişimli sistemde saklanması hâlinde, Tedarikçi bu bilgiyi Citi'ye ifşa etmelidir. Bu açıklama Hizmetlerin açıklamasına dâhil edilebilir. Tedarikçi, Citi Gizli Bilgilerini muhafaza ediyor veya saklıyorsa, bu Sözleşmenin süresi boyunca yılda bir kez SSAE 18 denetiminin (veya Citi tarafından onaylanan herhangi bir halef yetkili değerlendirmenin) yapılmasını sağlayacak ve yılda en az bir kez söz konusu SSAE 18 denetiminin veya Citi tarafından onaylanan herhangi

bir halef yetkili değerlendirmenin sonuçlarını belgeleyen raporların bir kopyasını Citi'ye sunacaktır.

16. Tedarikçinin herhangi bir birleşme, devralma veya benzer işlem kapsamında devralınması ya da başka bir tüzel kişiyi devralması ve söz konusu işlemin Hizmetleri etkileyebilmesi hâlinde Tedarikçi, Citi'yi derhâl yazılı olarak bilgilendirmeli ve devralma veya birleşmenin bu Gerekliliklere uyumu etkilememesini sağlamak için işlem sonucunda ortaya çıkan tüzel kişilik üzerinde bu Gerekliliklere uygun bir bilgi güvenliği değerlendirmesi yapmalıdır.

17.5 Alt Yüklenici Bilgi Güvenliği Riski

Tedarikçi, Citi gizli veya daha yüksek gizlilik derecesine sahip verilerine erişime sahip olan alt yüklenicilerin nitelikli Bilgi Güvenliği personeli tarafından yürütülen sözleşme öncesi ve periyodik sözleşme sonrası Bilgi Güvenliği (IS) değerlendirmelerini gerekli kılmasını şart koşmalıdır. Bu değerlendirmeler, başlangıçtan sorun yönetimine kadar değerlendirme sürecinin tüm aşamalarını kapsayan, yönetim tarafından onaylanmış bir sürece uygun olarak yapılmalıdır. Alt yüklenici IS değerlendirmesi, Citi'nin Üçüncü Taraf IS Değerlendirme Anketi'nde (TPAQ) yer alan IS alanları ile uyumlu IS alanlarında alt yüklenicinin duruşunu değerlendiren bir anket veya eş değer bir araçtan yararlanmalı ve alt yüklenicinin katılımıyla ilişkili IS riskini hesaplamak için mantıksal bir yöntem içermelidir. Tedarikçi, değerlendirmenin tamamlanmasını takip etmeli ve tespit edilen sorunları ve düzeltici eylem planlarını kapanışa kadar yönetmelidir.

17.6 Varlıkların Sorumluluğu

1. Tedarikçi, Citi Bilgisini saklamak, işleme almak ve/veya iletmek için kullanılan, kontrolü altındaki tüm uygulamalara ve donanıma ait envanterin tutulmasını sağlamalıdır.
2. Tedarikçi, Citi Bilgi varlıklarına ait herhangi bir envanterin, bu envanterin doğruluk ve tamliğini uygun şekilde sürdürmek için kullanılan bir sürece göre kendi kontrolü altında tutulmasını sağlamalıdır.
3. Tedarikçi kontrolü altındaki tüm Citi Bilgilerini korumaktan sorumlu olmalıdır.
4. Tedarikçi, endüstri uygulamaları ile tutarlı biçimde kullanıcılarının aktiviteye dair hesap verebilirliği sağlamalıdır.
5. Citi Bilgilerinin bulunduğu Tedarikçinin global ağında, haricî kişisel İnternet e-posta depolama ve bulut depolama hesaplarına kullanıcı erişimi kısıtlandırılmalıdır.

17.7 Bilginin Sınıflandırılması ve Kullanımı.

Citi, aşağıdaki Bilgi Sınıflandırması tablosuna göre bilgiyi sınıflandırır: Aşağıda listelenen her bir bilgi sınıflandırmasının tanımları ve örnekleri için Ek'e bakın.

KISITLI	En Hassas
HASSAS PII	
GİZLİ PII	
GİZLİ	
KURUM İÇİ PII	
KURUM İÇİ	
KAMUYA AÇIK	En Az Hassas

1. Citi Bilgilerinin sınıflandırmasına dayalı olarak, Citi, bu tür bilgileri korumak için gerekli güvenlik düzeyini belirlemek üzere Tedarikçiyle birlikte çalışmalı ve Tedarikçi, Citi'nin gerekli kılabilceği yükseltilmiş veya değiştirilmiş düzeylerle birlikte yeterli kontrollerin yürürlükte olmasını sağlamalıdır.
2. Kurum İçi veya daha yüksek gizlilik seviyesindeki bilgiler, Üçüncü Taraf ile Citi arasında, Citi politikaları ve standartları ile uyumlu gizlilik hükümleri içeren bir sözleşmeye tabi olan, Üçüncü Taraf yönetimindeki cihazlarda saklanmalıdır.
3. Tedarikçi Citi verilerinin depolanması için şirkete ait olmayan cihazların (ör., 4'üncü bir tarafın yönettiği cihazlar) kullanılmasına izin verirse, Tedarikçi, belirli yönetim onayını gerekli kılan bir politikaya ve Citi Bilgilerinin kullanılması ve elden çıkarılması için belirlenmiş kurallara ve izleme prosedürlerine sahip olmalıdır.
4. Tedarikçi, Citi Bilgilerini yetkisiz erişime, değişikliğe veya silmeye karşı her zaman korumalıdır.
5. Elektronik Taşınabilir Medya (ETM) aracılığıyla aktarılan Gizli veya daha yüksek olarak sınıflandırılan Citi Bilgileri, onaylanmış bir şifreleme algoritması kullanılarak şifrelenmeli ve teslimat onaylanmalıdır. Tedarikçi, ETM'nin amaçlanan kişi tarafından alındığını doğrulamalıdır. Alındı onayı beklenen teslimat tarihinde alınmadığı takdirde, Tedarikçi Citi'yi bilgilendirmelidir.

17.8 Güvenli Yapılandırma

1. Tedarikçinin Citi Bilgilerini depolama, işleme, erişme veya iletme potansiyeli olan tüm varlıklar için belgelenmiş bir güvenli yapılandırma standardı sürdürmesi gerekir.
2. Tedarikçi bilgi güvenliği kontrollerini, uygulamaların, ürünlerin ve hizmetlerin seçimi, geliştirilmesi ve uygulanması için kendi süreçlerine ve prosedürlerine dâhil etmelidir.
3. Tedarikçi, Citi Bilgilerinin saklandığı, işlendiği ve/veya iletildiği tüm sistemler için güvenli yapı prosedürüne sahip olmalıdır.
4. Tedarikçi, tüm sistemler için güvenli bir görsel veya şablon sürdürmelidir.
5. Tüm varsayılan kullanıcı hesapları ve parolalar satıcı tarafından desteklenen sistemlerden, ağ cihazlarından ve uygulamalarından kaldırılmalı ve/veya değiştirilmelidir.
6. Güvenliği ihlal edilen herhangi bir sistem veya hizmet, bütünlüğü kanıtlanmış bir görüntü veya şablon kullanılarak yeniden oluşturulmalı ve yapılandırılmalıdır.
7. Güvenli bir yapılandırmada yapılacak değişiklikler Tedarikçinin değişiklik yönetim süreci üzerinden yönetim tarafından onaylanmalıdır.

8. Tedarikçi, güvenli yapılandırmadaki herhangi bir değişikliği Citi'ye bildirmelidir.
9. Güvenli yapı prosedürü, üretim dağıtımı esnasında güvenlik/standart yapı ayarlarının otomatik yapılandırma denetimlerini destekleyecek araçları ve temel yapılandırmaya uyumun ve bunlardan sapmanın sürekli izlenmesini içermelidir.

17.9 Şifreleme Gereklilikleri

Tedarikçi, Gizli veya daha yüksek gizlilik dereceli bilgilerini şifrelenmemiş olarak iletmemelidir. Gizli veya daha yüksek gizlilik dereceli bilgiler, Citi onaylı araçlar veya çözümlerle **uçtan uca** şifrelenmelidir. Verilerin şifrelenerek iletimine yönelik onaylanan protokoller ve ilgili sürüm numaraları aşağıdaki gibidir:

1. Kimlik doğrulama ve yetkilendirme bilgilerinin değişimi sırasında: SAML v2.0, OAuth v2.0 (yalnızca yetkilendirme),
2. İletişim kanallarını ve ilgili anahtar alışverişini korumak için yalnızca aşağıdaki Ağ Güvenliği Protokollerine izin verilir:
 - a) TLS v1.3 tercih edilir ve tüm TLS v1.3 paketlerine izin verilir. Etkin olan tek protokolün TLS v1.3 olması durumunda ek inceleme gerekmez.
 - b) TLS v1.3 teknik olarak uygulanabilir değilse ve TLS 1.2 kullanılıyorsa SSLabs'tan B veya daha yüksek bir not şu anda kabul edilebilir ve ek inceleme gerekmez.

Citi Üçüncü Taraf ortamında kalıcı olarak saklanan veya değiş tokuş edildiğinde veriler, Citi onaylı araçlar veya çözümler kullanılarak tamamen şifrelenmelidir. Verileri şifrelemek için onaylanmış algoritmalar ve anahtar uzunlukları aşağıdaki gibidir:

1. **Advanced Encryption Standard (AES):** Onaylı anahtar uzunlukları: 256 veya daha fazla bit. Kısıtlı Modlar: Elektronik Kod Kitabı (ECB) modu, düz metin miktarının blok uzunluğundan küçük veya ona eşit olduğu durumlar dışında yasaktır. Disk sürücüsü şifrelemesi: 256 bit anahtarlı AES gereklidir. 128 bit anahtar uzunluğuna sahip AES'e TLS şifre paketi seçeneği olarak izin verilir; ancak Citi'nin uluslararası takvimlerle uyumunu sağlamak amacıyla bu seçeneğe 31 Aralık 2028 itibarıyla 256 bit veya daha yüksek güç lehine artık izin verilmeyecektir (Bkz. NIST 8547 IPD).
2. **ChaCha20 (ilişkili kullanım durumları için bir akış şifresi):** Onaylı anahtar uzunlukları: 128 veya 256 bit, 96 bitlik nonce ve 32 bitlik blok sayısı veya 64 bitlik nonce ve 64 bitlik blok sayısı. Maksimum veri boyutu: 16 petabayt.

Onaylanmış açık anahtarlı kriptosistemleri, anahtar değişimi, anlaşma mekanizmaları, mesaj özeti ve anahtar türetme fonksiyonları şunlardır:

Tedarikçinin Kuantum Hazırlığına İlişkin Bildirim: Tedarikçiler, NIST IR 8547 (ipd) *tablo 2* ve *tablo 4* kapsamına ilişkin planlarını ([survey link](#)) aracılığıyla Citi Quantum Readiness Program ekibine sunmalıdır.

1. **Açık Anahtar Kriptosistemleri ve minimum anahtar uzunluğu boyutları:**
 - a) Rivest – Shamir – Adleman (RSA): 2048 bit.
 - b) Dijital İmza Algoritması (DSA): 2048 bit. DSA, Citi dışında işlenen veya saklanan Citi verilerinin güvenliğini sağlamak için kullanılmamalıdır.

- c) Eliptik Eğri Dijital İmza Algoritması (ECDSA): 256 bit ve NIST tarafından önerilen eğrilerle ANSI X9.62'de belirtildiği gibi.
- 2. **Anahtar Değişimi ve Anlaşma mekanizmaları ve minimum anahtar uzunluğu boyutları:**
 - a) Diffie-Hellman (DH)/Geçici Diffie-Hellman (DHE): 2048 bit.
 - b) Eliptik Eğri Diffie-Hellman (ECDH)/Geçici Eliptik Eğri Diffie-Hellman (ECDHE): 256 bit ve NIST tarafından önerilen eğrilerle ANSI X9.63'te belirtildiği gibi¹.
- 3. **Mesaj Özeti İşlevleri:** Hash oluşturmak için kullanılan malzemede rastgele bitlerin sayısından daha uzun bir şifreleme anahtarı oluşturmak yasaktır.
 - a) SHA-1 yalnızca dijital imza uygulamaları dışındaki uygulamalarda kabul edilebilir. SHA-2 ailesi, SHA-3 ailesi ve POLY-1305: Tüm kriptografik karma fonksiyonu uygulamaları için kabul edilebilir.
- 4. **Parola Tabanlı Anahtar Türetme Fonksiyonları ve Minimum Gereklilikler:**
 - a) PBKDF2: En az 16 baytlık bir tuzla en az 10000 yineleme sayısı.
 - b) HKDF: Tuzlanmalı ve bilgi giriş değeri dâhil edilmelidir.
 - c) SCRYPT: Minimum tur sayısı/maliyet faktörü 10.
 - d) NIST SP800-108 KDF'nin Akış Şifrelemesi için kullanılması yasaktır. NIST SP 800-108 KDF Modes, yani Counter, Feedback ve Double-Pipeline Iteration modları kabul edilebilir.
 - e) Argon2 önerilir.
- 5. **Parola karma işlevleri ve asgari gereklilikler:**
 - a) Bcrypt (kimlik doğrulama materyalinin yerel olarak saklanması için): Minimum tur sayısı/maliyet faktörü en az 10.
 - b) Herhangi bir Tedarikçi ürünü tarafından dağıtılan ortamlarda veya sistemlerde parolaları yerel olarak saklarken parola karma işlemi için Argon2 veya PBKDF2 önerilir.

17.10 Harici E-posta

Tedarikçinin regülasyon ve/veya Tedarikçi politikası uyarınca Citi onaylı uçtan uca şifreleme yazılımı veya araçlarını kullanmasına izin verilmeyen durumlarda, Gizli veya daha yüksek Citi Bilgi sınıflandırmasına sahip Citi Bilgilerini içeren münferit e-postalara ilişkin şifreleme gerekliliği, aktarım şifrelemesiyle [ör., Transport Layer Security (TLS) aracılığıyla ağ geçidinden ağ geçidine şifreleme] tamamen karşılanabilir. Onaylanmış güvenli E-posta protokolleri şunlardır:

1. **Identify-Based Encryption (IBE)**, e-posta şifreleme özelliği sunar ve yalnızca Citi'nin müşteriye dönük çözümlerinde, güvenli e-posta sistemlerinde ve eDelivery sistemlerinde kullanılabilir.
2. **Mandatory TLS (MTLS)**, oturum şifreleme özelliği sunar (e-posta yükünü şifrelemez) ve kullanımı için önceden anlaşma yapılmış satıcılar, iş ortakları ve müşterilerle kullanılabilir.
3. **Domain Keys Identified Mail (DKIM)**, kaynak kimlik doğrulama ve anahtar yönetimi özellikleri sunar ve satıcılar, iş ortakları ve müşterilerle kullanılabilir.

¹ ECDHE tercih edilir.

17.11 Özel Ağlar

Tanınmış bir otorite tarafından bağımsız biçimde düzenlenen ve lisanslı ve akredite karşı taraflar arasında işin yapılmasına ilişkin bir Finansal Hizmetler Endüstri standartlarını (ör., SWIFT veya bir merkez bankası) karşılayan özel ağlar, bu ağların şifreli iletimleri tam anlamıyla desteklemek için gerekli alt yapıyı sağlayana kadar transit Gizli PII şifreleme gerekliliğinden muaf olarak değerlendirilirler.

17.12 Ses ve Faks

Faks üzerinden gönderilen veya sesli çağrılarda (Voice Over IP [VOIP] dâhil) görüşülen Gizli veya Daha Üst Düzey Citi sınıflandırmasına sahip bilgiler şifrelenmemiş olarak gönderilebilir. Gerektiğinde, Tedarikçi bu kanallar yoluyla Gizli veya daha üst düzey gizlilik derecesine sahip bilgileri korumak için belirli prosedürleri ve rehberliği geliştirmelidir.

17.13 Kriptografik Anahtar ve Sertifika Yönetimi

Bu maddede kullanılan güvenli sınır terimi, Federal Information Protection Standard (FIPS) gibi bir Cryptographic Module Validation Program (CMVP) tarafından doğrulanmış sınırı ifade eder (kabul edilebilir asgari güvenlik düzeyi FIPS 140-2/3 Level 2'dir). (AWS Nitro Enclave'leri gibi Gizli Hesaplama Enclave'leri kabul edilebilir. Diğer benzersiz güvenlik sınırı durumlarının Citi tarafından onaylanması gerekir).

1. Tedarikçi, şifreleme ve imzalama (SSH anahtarları dâhil) için güncel endüstri standardı kriptografik algoritmaları ve asgari anahtar uzunluklarını kullanmalıdır. Tedarikçi, söz konusu algoritmalar ve anahtar uzunlukları endüstri standartlarıyla uyumlu olacak şekilde güncellendiğinde, Değişiklik Yönetimi Süreci aracılığıyla güvence sağlamalıdır.
2. Tedarikçi, hassas materyalleri yetkisiz kullanım veya ifşadan korumak için kontrollerin bulunduğu resmî, belgelenmiş bir anahtar, sır ve sertifika yönetimi yaşam döngüsü sürecine sahip olmalıdır. Tüm kriptografik sırlar ve anahtar yaşam döngüsü olayları yalnızca güvenli bir sınır içinde gerçekleşmelidir. Ayrıcalıklı ve güvenli sınırlara tüm erişimler belgelenmelidir. Tedarikçi, ilgili aktörleri, birimleri ve sınırları vurgulayan tüm anahtar yaşam döngüsü olayları için bir sıra diyagramı sağlamalıdır.
3. Kriptografik Anahtarların benzersiz bir amacı olmalıdır ve asla, disk şifreleme ve veri şifreleme için aynı şifreleme anahtarının kullanılması veya veri şifrelemenin yanı sıra veri tabanı şifreleme için aynı şifreleme anahtarının kullanılması gibi başka herhangi bir amaç için kullanılmamalıdır. Bir SaaS tedarikçisinin birden fazla kiracı arasında kriptografik anahtarları yeniden kullanması varsayılan olarak yasaktır ve yalnızca Gizli PII, Hassas PII ve Kısıtlı sınıflandırmalarının altında yer alan Citi Bilgilerini içeren kritik olmayan, düşük riskli kullanım senaryoları için, Security Architecture Council'in açık onayına tabi olarak izin verilebilir.
4. Tüm kriptografik anahtarlar (simetrik veya asimetrik) için, özel anahtar veya özel anahtar malzemesi (tohumlar veya özel anahtarın bir kısmı gibi) hiçbir zaman açık metin olarak görüntülenmemelidir. Özel anahtar veya özel anahtar malzemesi (tohum veya özel anahtarın bir kısmı gibi), dinamik oturum anahtarları gibi geçici anahtarlar haricinde asla güvenli sınırdan ayrılmamalıdır. Tasarım, güvenli bölgeler/ayrıcalıklı erişim sınırları arasında

simetrik anahtar veya özel anahtar malzemesinin iletilmesini gerektiriyorsa, yalnızca karşılıklı TLS şifreli tüneller aracılığıyla yalnızca Simetrik Anahtar Sarma Anahtarı veya Genel Anahtar Taşıma Anahtarı kullanılarak şifrelenmiş biçimde iletilmelidir ve bu tür bir iletim Citi tarafından yazılı olarak onaylanmalıdır. Özel Anahtar Taşıma Anahtarı bu durumlarda oluşturulduğu ayrıcalıklı erişim güvenli sınırından hiçbir zaman ayrılmamalıdır.

5. Simetrik Anahtar Sarma Anahtarı, iki veya daha fazla anahtar bileşene bölünmeli ve dağıtılmadan önce ve manuel anahtar girişi/yüklemeye için XOR'lanmalıdır. Simetrik Anahtar Sarma Anahtarı, CMVP doğrulanmış modüller gibi güvenli sınırın içinde ilişkilendirilmiş yeterli Erişim Kontrol Listelerine (ACL'ler) sahip olmalıdır ve Simetrik Anahtar Sarma Anahtarı güvenli sınırın dışında saklanmamalıdır.
6. Özel anahtarlar veya sırlar veya özel anahtar materyali (tohum veya özel anahtarın bir kısmı gibi) içeren anahtar depolarına veya güvenli sınırlara insan veya hizmet veya otomatik aracı erişimi, erişimi yalnızca yetkili personel veya sistemlerle sınırlayan kontrollerle uygun şekilde ayrılmalıdır.
7. Özel veya simetrik anahtarlar içeren anahtar depolarına erişim için yapılan her istek, denetim amacıyla erişimin kim, ne zaman ve ne amaçla yapıldığı gibi ayrıntılarla günlüğe kaydedilmeli ve belgelenmelidir.
8. Tedarikçi kendinden imzalı ve joker karakterli sertifikalar veya varsayılan SSL sertifikaları kullanmamalıdır.
9. Tüm kriptografik Anahtarlar, NIST SP800-57 bölüm 1, revizyon 6'da önerildiği gibi tanımlanmış bir kriptoperiyot zaman aralıklarına sahip olmalıdır. Değişiklik dönemleri, zamanlama çakışmaları ve sistem donmalarına uyum sağlamak için anahtarlar süre sonunda önce yenilenmeli veya değiştirilmelidir.
 - a) Süresi dolmuş bir sertifikayı değiştirirken eski asimetric anahtar çiftinin yeniden kullanılması yasaktır.
10. Kriptografik Anahtarların bütünlüğünün, anahtarın saklandığı veya paylaşıldığı ortamın veya simetrik veya özel anahtarın gizliliğinin ihlal edildiğinden şüphelenildiği anda anahtarlar tehlikeye atılmış olarak değerlendirilmelidir. Tehlikeye maruz kalan tüm anahtarlar operasyonel kullanımdan kaldırılmalı ve ilgili tüm sertifikalar iptal edilmelidir.
11. Kablosuz ağlar, endüstri standardında şifreleme algoritmalarıyla şifrelenmelidir.
12. Kriptografik mekanizmanın herhangi bir şeklini kullanan tedarikçiler, endüstri standardı anahtar yönetim araçlarını ve tekniklerini kullanmalıdır. Anahtar yönetimi rolü operasyonel yönetimden ayrılmalıdır.
13. Tedarikçiler, yalnızca Citi Veri Güvenliği Hizmetleri tarafından sağlanan PKI ve KMS hizmetleriyle birlikte çalışabilirlik sağlandığı ve kriptografik kontrol Citi kriptografik yönetişiminin dışına devredilmediği durumlar dâhilinde buluta özgü KMS ve PKI çözümlerinden yararlanabilir.

17.14 Erişim Kontrolü Sorumluluğu

Citi Gizli veya daha yüksek Bilgilerini depolamak, erişmek, yönetmek, işlemek veya iletmek için kullanılan tüm Kontrollü Bilgi Sistemlerini yetkisiz erişime karşı korumak için Tedarikçi, kullanıcı yetkilerini her iş fonksiyonu için gereken asgari erişim düzeyiyle sınırlandırarak ve tüm sistem ve uygulamalara mantıksal erişimin sağlanmasını

yöneterek en az ayrıcalık ilkesini uygulamaktan sorumludur. Kontroller tamamen belgelendirilmeli ve denetlenebilir olmalıdır. Parola sıfırlama ve etkinleştirme dâhil olmak üzere erişim tanımlama ve kaldırma işlemleri, insan hatasından kaynaklanabilecek olası aşırı yetkilendirme riskini azaltmak ve sektör standartlarıyla uyum sağlamak amacıyla mümkün olan her durumda otomatik bir süreç üzerinden gerçekleştirilmelidir.

1. Tedarikçi, organizasyonundaki tüm kullanıcıların erişim haklarından sorumludur.
2. Tedarikçi, kullanıcılara yalnızca görevlerini yerine getirmeleri için kesinlikle gerekli olan ayrıcalıkların ve hakların verilmesini sağlayan erişim kontrolleri uygulamalıdır.
3. Tedarikçi yetkisiz kullanımı önlemek için tüm varsayılan erişim kabiliyetlerinin kaldırılmasını, devre dışı bırakılmasını veya korunmasını sağlayacak bir süreci uygulamalıdır.

17.15 Kullanıcı Erişim Yönetimi

Tedarikçi, Citi Gizli veya daha yüksek gizlilik derecesine sahip bilgileri işleyen, depolayan ve/veya ileten sistemlere ve uygulamalara mantıksal erişim teminini yönetmelidir. Şunları içerir:

1. Onaylı kimlik doğrulama sistemlerinin tanımlanması ve envanteri.
2. Citi verilerine tüm erişimin bir müdürden veya müdürün tayin ettiği kişiden ve sistemin sahibinden onay gerektirmesine yönelik bir gereklilik. Tedarikçi, Citi verilerine erişimi olan herhangi bir personeline, bilmesi gerekenler temelinde bu tür bir erişim izni verilmesini sağlamaktan sorumludur.
3. Bireysel bir kullanıcı için herhangi bir ayrıcalık/işlev kombinasyonunun/birleşimlerinin, çıkar çatışması veya yapıcı-denetleyici kurallarının ihlaline yol açması durumunda sağlanmamasına ilişkin bir gereklilik.
4. Sistemdeki her kullanıcıya verilen/geri alınan erişim haklarını gözetmek ve yönetmek için bir izleme süreci.
5. Erişim taleplerinde başka bir kullanıcının yetkilerinin kopyalanması/klonlanması yöntemine başvurulmamalıdır; yetki birikimini önlemek ve en düşük yetki prensibini uygulamak amacıyla taleplerde, iş gerekçesiyle birlikte açıkça belirtilmiş roller/yetkiler yer almalıdır.

17.16 Kullanıcı Kimliği Saptama ve Doğrulama

Tüm Tedarikçi kontrollü Bilgi Sistemleri, Citi Bilgilerine erişimin sağlandığı bir oturum veya işlem başlatılmadan önce bu platformlara erişen kullanıcıların veya sistemlerin kimliğini doğrulamalıdır.

1. Kullanıcılar benzersiz biçimde tanımlanmalı veya bir Kullanıcı ID yoluyla teknoloji platformuna eşlenmelidir.
2. Kullanıcıların teknoloji platformunda onaylı bir kimlik doğrulama yöntemi kullanılarak kimliği doğrulanmalıdır. Tedarikçi, mevcut onaylı yöntemler için birincil iş iletişim kişisi (BAO) ile iletişime geçmelidir.

3. Paylaşılan kimlik doğrulama altyapısının (ör., Tek Oturum Açma, Azaltılmış Oturum açma ve diğer paylaşılan Citi kimlik doğrulama hizmetleri) tüm kullanımları kimlik doğrulama gerekliliklerine uygun olarak olmalıdır; Tedarikçi mevcut onaylı yöntemler için birincil BAO ile iletişime geçmelidir.
4. Bir kullanıcının bir Bilgi Sisteminde kimliğini doğrulamak için kullanılan Kimlik Doğrulama Verilerinin (IVD), iletim ve depolama sırasında şifrelenmesi gerekir. Şifreleme gereklilikleri için bölüm 17.9'a bakın.
5. Tedarikçi personelinin Citi sistemlerine erişmek için kullandığı her hesap, benzersiz ve Citi tarafından atanan bir tanımlayıcıyla (ör., GEID) eşleştirilmelidir; izlenebilirliği, SOD uygulamasını ve denetime hazırlığı sağlamak amacıyla gerçek kullanıcılar için genel/paylaşımlı kullanıcı kimlikleri yasaktır.

17.17 Ayrıcalıklı Erişim Kimliklendirmesi ve Geçici Ayrıcalıklı Erişim

Tedarikçi, tüm kimliklerin bir envanterini tutmalı ve ayrıcalıklı erişime sahip olanlar ile Gizli PII veya Üstü olarak sınıflandırılmış bilgiler içeren elektronik depolara (ticari uygulamaları destekleyen veri kümeleri veya veri tabanları) erişimi bulunan kimlikleri belirlemelidir. Tedarikçi, bu Kimliklerin yetkisiz kullanımına karşı koruma sağlayan kontroller uygulamalıdır. Bir çalışanın ayrıcalıklı bir kimliğe veya daha önce belirtilen elektronik depolara erişmesi gerekiyorsa erişim, aşağıdakileri sağlayan geçici bir erişim yönetimi süreci aracılığıyla verilmelidir:

1. Talep edenin önceden onaylı bir yetkili kullanıcılar listesinde olmasını veya kullanım anında bir onay edinmesini gerektirir.
2. Erişim verilmeden önce bir değişiklik/sorun biletinde gerekçenin belgelendirilmesini gerektirir.
3. Erişimle gerçekleştirilen aktivitenin bağımsız bir incelemesini içerir.
4. Geçici erişim süresinin sonunda erişimin iptal edilmesi / kaldırılması sürecini başlatmayı kapsar.
5. Örneğin büyük yükseltme veya kesinti/onarım çözümünden sonra üretim ve uygulama sonrası stabilizasyon erişiminin yedi (7) takvim gününe kadar uzatılmasına izin verir.

17.18 Kullanıcı Erişim Haklarının İncelemesi

1. Tedarikçi, en az yılda iki kez Citi Bilgilerini saklamak, işlemek, yönetmek ve/veya iletmek için kullanılan Kontrollü Bilgi Sistemine gereksiz kullanıcı yetkilendirmelerini incelemek, doğrulamak ve silmek için belgelendirilmiş bir süreç uygulamalıdır.
2. Kullanıcılar, kendi yetkilerini veya inceleme sorumluluğunu kendilerine devreden bir kişinin yetkilerini incelememeli veya onaylamamalıdır.
3. Citi dâhilinde bir Tedarikçi çalışanı tarafından fonksiyon değişikliğini takiben, Tedarikçinin bir erişim ve yetkilendirme incelemesi yapmak ve çalışanın yeni fonksiyonları için artık gerekmiyorsa Citi verilerine erişimi kaldırmak için 14 takvim günü zamanı vardır.

17.19 Güvenli Oturum Açma Prosedürleri

1. Kilitlenen kullanıcı oturum açma kimlikleri, endüstri standardında bir sıfırlama hizmeti veya başka bir yetkili işlev aracılığıyla yeniden

etkinleştirilmelidir. İşletim sistemi veya uygulama tarafından desteklendiğinde, kullanıcının ilk kez oturum açtığı veya kimliğinin doğrulandığı tüm ağ giriş noktalarında bir başlık metni görüntülenmelidir.

17.20 Parola Yönetim Sistemi

1. Kullanıcı statik şifreleri hiçbir zaman ekranda açık metin olarak görüntülenmemelidir. Aşağıdaki koşulların sağlanması kaydıyla, parola görünürlüğünü değiştirme işlevi bu gereklilikten muaftır:
 - (1) Parola girişi varsayılan olarak maskelenmelidir,
 - (2) Parolanın görünürlüğü yalnızca kullanıcının açık bir eylemiyle başlatılabilmelidir,
 - (3) Kullanıcı eylemi sona erdikten sonra en fazla 15 saniye içinde parola otomatik olarak yeniden maskelenmelidir.
2. Ayrıcalıklı İşlevsel Kimlik parolaları açık metin olarak sabit kodlanmamalıdır.
3. Statik parolalar hem harf hem rakam içermeli, büyük-küçük harfe duyarlı olmalı ve en az on (10) karakterden oluşmalıdır. Statik parolaların büyük/küçük harf duyarlılığı her kimlik doğrulama noktasında doğrulanmalıdır. Fonksiyonel Kimliklerin (FID) statik parolaları, 31 Ağustos 2026 tarihinden sonra kullanıma sunulan uygulamalarda en az 15 karakter içermelidir.
4. PIN'ler, yalnızca fiziksel cihaz kısıtlamalarını (örneğin tuş takımı, telefon, akıllı kart) karşılamak için PIN'lerin gerekli olması durumunda, Bilgi Sistemlerine erişim için tek kimlik doğrulama yöntemi olarak kullanılabilir.
5. Tüm statik şifreler en az 90 takvim gününde bir değiştirilmelidir.
6. Art arda en fazla altı (6) başarısız oturum açma denemesi veya art arda en fazla altı (6) parola sıfırlama denemesinden sonra tüm statik parolalar kilitlenmelidir. Parolaların kilidi bir kimlik yöneticisi işlevi aracılığıyla veya en az 30 dakika sonra otomatik olarak açılmalıdır.
7. Tüm kimlik doğrulama sistemleri, 100 takvim gününü geçemeyecek bir oturum açma/kullanmama kontrolü uygulamalıdır. Teknik olarak mümkünse, devre dışı kalan oturumlar, kullanıcı veya diğer yetkili fonksiyon tarafından yeniden etkinleştirilebilir.
8. Kimlik doğrulama süreci, en azından en son altı (6) değişiklikte aynı parolanın kullanılmamasını sağlamalıdır.

17.21 Sistem Yardımcı Araçlarının Kullanımı

Tedarikçi sistemi ve uygulama kontrollerini (ör., çevre cihazlardan başlatma) devre dışı bırakabilecek yardımcı programların kısıtlı ve kontrollü kullanımını sağlamalıdır.

17.22 Oturum Zaman Aşımı

1. Citi Bilgilerini depolamak, işlemek ve/veya iletmek için kullanılan Kontrollü Bilgi Sisteminin tüm kullanıcıları için oturum açma ve yeniden kimlik doğrulama işlemi gerçekleştirilmelidir.
2. Kullanıcıların, 30 dakikayı aşmayan bir süre işlem yapılmaması durumunda yeniden kimlik doğrulaması yapması gerekir. İşlem, uç noktaya (fare, klavye, dokunmatik ekran vb.) yapılan her türlü girişi içerir. Uygulamanın parola korumalı ekran koruyucu tarafından sağlandığı durumlarda, Uygulama/Tek Oturum Açma zorunluluğu gerekli değildir.

17.23 Kullanıcı Erişiminin Sonlandırılması

1. Fesih veya istifa sonrasında, Masaüstü/Etkin Dizin kullanıcı oturum açma, Tek Oturum Açma (SSO), e-posta, Tek Kullanımlık Şifre (OTP) belirteçleri ve uzaktan erişim dâhil olmak üzere Citi Gizli veya daha yüksek gizlilik seviyesindeki verilere erişime izin verebilecek kullanıcı erişimi ve yetkilendirmeleri derhâl kaldırılmalıdır.
2. Bir çalışanın Citi'nin sahip olduğu ve yönettiği sistemlere erişimi varsa, Citi İşletme Müdürünün işten çıkarılan çalışanlar için erişimin sona erme tarihinin sonuna kadar şirket tarafından kaldırılmasını başlatmasını sağlamak amacıyla, o çalışanın görev değişikliği veya işten çıkarılması üzerine Citi İş İlişkileri Yöneticisi, BAO veya BAO desteği derhâl bilgilendirilmelidir.
3. Tedarikçi, bir çalışanın veya çalışan olmayan kişinin işine son verildiğinde veya istifa ettiğinde bölüm 17.23.2'de belirtilen zaman dilimleri doğrultusunda tüm varlıklardan erişimi geri almak için belgelenmiş bir sürece sahiptir.
4. Tedarikçi tarafından 17.23.1-17.23.3 ile ilgili olarak herhangi bir anormallik tespit edilirse tedarikçi, sağlam bir gerekçe ve sağlanan kontrollerle birlikte Citi İş İlişkileri Yöneticisini, BAO'yu veya BAO desteğini derhâl bilgilendirmelidir.

17.24 Uzaktan Erişim

Tedarikçi, aralarında aşağıdakilerin yer alabileceği Citi Gizli veya daha yüksek gizlilik derecesine sahip verileri depolayabilecek, işleyebilecek veya iletebilecek ağlara erişimi korumak için uzaktan erişim denetimlerine sahip olmalıdır:

1. Citi Bilgilerini saklamak, yönetmek, işlemek ve/veya iletmek için kullanılan Bilgi Sistemlerine uzaktan erişim yetkisiz kullanıma karşı korunmalıdır.
2. Citi Bilgilerini saklamak, işlemek ve/veya iletmek için kullanılan, Tedarikçi tarafından yönetilen tüm dizüstü ve masaüstü bilgisayarlar; ayrıca Gizli veya daha yüksek Citi Bilgi sınıflandırmasına sahip bilgilerin yerel olarak saklandığı/işlendiği uzaktan erişim kullanımında, endüstri standartlarını karşılayan bir şifreleme aracıyla şifrelenmelidir.
3. Uzaktan bağlantılar yalnızca çok faktörlü kimlik doğrulaması (MFA) kullanan onaylı uzaktan erişim çözümleri üzerinden kurulmalıdır.
4. Tedarikçi tarafından yönetilen makineler, İnternet'e doğrudan bağlandıklarında (diğer deyişle, tedarikçi tarafından yönetilen bir güvenlik duvarı veya proxy yoluyla değil) etkin bir kişisel güvenlik duvarına sahip olmalıdır.
5. Tedarikçi tarafından yönetilen cihazlar, ağa tam erişim için bir gereklilik olarak düzenli yazılım/antivirüs araçlarının güncellemelerini almak ve yüklemek için tedarikçi ağına düzenli şekilde bağlanmalıdır. Sınırlı erişime yalnızca cihazın güncellenmesi amacıyla izin verilmelidir.
6. Citi Gizli veya daha yüksek gizlilik derecesine sahip bilgilere erişmek için Tedarikçinin sahip olmadığı ve yönetmediği cihazlar kullanılıyorsa, yerel makineye indirmeye izin vermeyen yetkili bir çözüm kullanacak şekilde yapılandırılmalıdırlar. Aşağıdaki kontroller mevcut olmalıdır:
 - a) Citi Verilerinin şirket tarafından yönetilen bir çözüm dışında cihaza indirilmesi önlenir.
 - b) Tedarikçi, söz konusu erişimin standart uzaktan erişim teknolojileri [ör., Virtual Desktop Interface (VDI)] kullanılarak belirteç tabanlı veya

sertifika tabanlı kimlik doğrulamayla güvence altına alınmasını sağlamalıdır.

- c) Terminal Services ve VMware Horizon gibi uzaktan erişim çözümleri; Blast ve PCoIP üzerinden pano paylaşımını ve sürücü eşlemeyi, ayrıca RDP ve SSH protokollerini devre dışı bırakacak şekilde yapılandırılmalıdır.
7. MFA için yazılım belirteçleri kullanılıyorsa, örneğin bir mobil cihazdaki yazılım uygulamasına erişmek için, yazılım belirteci kimlik doğrulama yazılımı kullanıcının kimliğini doğrulamalıdır (ör., parola, biyometrik, vb. ile) ve cep telefonu jailbreak'li veya root'luysa (mobil cihaz satıcısı tarafından onaylanan ve sağlananlar dışında bir işletim sistemi kullanarak) kullanımını engellemelidir.
8. Sistemler, veri depoları, uygulamalar ve/veya altyapı için özel, ayrıcalıklı ve/veya yönetici düzeyinde erişim gerektiren; sistem yöneticileri, veri tabanı yöneticileri, erişim kontrolü yöneticileri, güvenlik duvarı yöneticileri ve web sitesi yöneticileri dâhil ancak bunlarla sınırlı olmamak üzere, Citi'ye sağlanan Hizmetlerle doğrudan veya dolaylı olarak ilişkili tüm daimi/geçici çalışanlar, yükleniciler ve alt yükleniciler yalnızca MFA ile doğrulanmalı; söz konusu erişim, bu Gerekliliklere uygun olarak şüpheli aktivite ve/veya yetkisiz erişim açısından Tedarikçi tarafından bağımsız biçimde günlüğe kaydedilmeli ve izlenmelidir.
9. Kişisel olarak sahip olunan cihazlar ve bir üçüncü tarafın sahip olduğu cihazlar için Tedarikçi, bu tür cihazların ağ üzerinde oturum açmasına izin verilmesi için öncelikle bu cihazların onaylı bir işletim sistemi sürümüne, yama düzeylerine, virüsten koruma ve kötü amaçlı yazılımdan koruma çözümlerine sahip olmasını sağlayacak etkili bir çözüme sahip olmalıdır.
10. Tedarikçi, tüm personelinin aşağıdaki hususları yerine getireceğinden emin olmalıdır:
 - a) Herhangi bir sesli asistan cihazı (ör., Siri, Alexa), video kayıt cihazı ve/veya diğer fotoğraf, video ya da ses dinleme/kayıt cihazlarını içermeyen, kişiye özel ve ayrılmış bir uzaktan çalışma alanını sürdürecektir. Yetkisiz personelin, uzak bilgi işlem sistemlerinin ekranlarında görünebilecek herhangi bir veri, sistem ve uygulamayı görüntülemesine izin verilmeyecektir.
 - b) Ekranı görüntülemek için yetkisiz erişimin yeterince azaltılmasını sağlamak için cihazı gözetimsiz bırakırken bilgi işlem cihazını kilitleyecektir.

17.25 Temiz Masa Politikası

Tedarikçi personeli, kendi iş alanlarında kullanılan veya saklanan fiziksel bilgi dâhil olmak üzere her türlü Citi Bilgisini korumak zorundadır. Tedarikçilerin bu gerekliliği IS eğitimi veya başka bir kanal yoluyla personeline en azından yıllık olarak iletmesi gerekir.

17.26 Yangın Güvenliği

1. Tedarikçi, yerel yangın kuralları da dâhil olmak üzere, fiziksel güvenlik ve güvenli bir çalışma ortamının oluşturulmasıyla ilgili geçerli yasal ve düzenleyici gerekliliklere uymalıdır.
2. Tedarikçi bir yangın tespit, alarm ve baskılama sistemi/sistemleri kullanmalıdır. Sistemler altı ayda bir denetlenmeli ve yıllık olarak test edilmelidir.

17.27 Fiziksel Güvenlik

1. Citi Bilgileri, erişimi sadece yetkili personel ile sınırlandıran kontrolleri içeren güvenli alanlarda saklanmalıdır.
2. Tedarikçi, belgelendirilmiş ve denetlenebilir bir fiziksel erişim kontrol sistemine sahip olmalıdır.
3. Tedarikçi, ortama ve sağlanan hizmetlere uygun olarak, üçüncü bir tarafça izlenen güvenlik alarmini, güvenlik görevlilerini ve video gözetimini içeren güvenlik alarmı/izinsiz giriş sistemlerinin bir kombinasyonunu kullanmalıdır.
4. Tedarikçi, tüm ziyaretçilerin varışta doğrulanabilir kimlik göstermesini ve giriş-çıkış kaydı yapmasını gerektiren, belgelenmiş bir ziyaretçi politikasına sahip olmalıdır.

17.28 Operasyonel Güvenlik Prosedürleri ve Sorumluluğu

1. Tedarikçi değişiklik yönetimi süreci, değişikliğin kaydedilmesi, gözden geçirilmesi, test edilmesi, onaylanması, uygulanması ve kapatılmasıyla ilgili temel kontrol noktası kontrollerini içermelidir. Tedarikçinin ayrıca zorunlu onaylar hiyerarşisi de dâhil olmak üzere listelenen tüm aşamaları gerektiren bir acil durum değişiklik sürecine sahip olması gerekir.
2. Tedarikçinin kapasite yönetimi konusunda kullanılabilirliği, kapasiteyi ve performans ölçümlerini/göstergelerini; iş etki değerlendirmesini; performans ve kapasite sorunlarını proaktif izleme, araştırma ve ele almayı içeren (ancak bunlarla sınırlı olmayan) denetlenebilir bir süreci olması gerekir.
3. Geçerli olduğu durumlarda Tedarikçi, Laboratuvar, Geliştirme, Test ve Üretim ortamlarının tamamının fiziksel ve/veya mantıksal olarak birbirinden ayrıldığından emin olmalıdır.

17.29 Yazılım Geliştirme Gereklilikleri

Citi'nin özel kullanımı için geliştirilen yazılımları sunan Tedarikçiler için geçerlidir. Tedarikçiler bu gerekliliklere uymalı veya eş değer yaklaşım ve kalitede, belgelenmiş ve onaylanmış bir Software Development Lifecycle ("SDLC") süreci sunmalıdır.

17.30 Başlatma ve Planlama

Tedarikçi, çözümün kapsamını ve hedeflerini Citi'nin gerekliliklerine ve sözleşme yükümlülüklerine uygun olarak tanımlamalıdır. Şunları içerir:

1. Fonksiyonel ve işlevsel olmayan gerekliliklerin belgelenmesi;
2. Efor ve zaman çizelgesi tahminlerinin sunulması; ve
3. Tüm üçüncü taraf bileşenlerinin veya bağımlılıklarının belirlenmesi.

Güvenlik riski değerlendirmeleri de dâhil olmak üzere uyum aktiviteleri proje başlangıcında başlatılmalıdır. Roller, sorumluluklar ve onay kontrol noktaları açıkça iletilmelidir.

Tüm ortamlar Geliştirme (DEV), Test (TEST) veya Üretim (PROD) olarak sınıflandırılmalı ve yaşam döngüsü boyunca kesin bir şekilde ayrılmış olarak kalmalıdır. Ortam sınıflandırması, erişim izinlerini ve işlenebilecek veri türünü belirler. Tedarikçi, yetkisiz erişimi veya veri ifşasını önlemek amacıyla erişimleri ortam tanımına göre sınırlandırmalı ve dağıtımları uygun SDLC aşamasının tamamlanmasıyla uyumlu hâle getirmelidir.

17.31 Tasarım

Tedarikçi, teslim edilen çözümün belirtilen tüm gereklilikleri karşılmasını sağlayan bir tasarım yaklaşımını belgelemelidir (bir "Test Planı"). Bir Test Planı en azından aşağıdakileri içermeli ve açıklamalıdır:

1. Gerekliliklere izlenebilirlik sağlayan, birim testleri ile işlevsel ve işlevsel olmayan testler ve performans yönü testleri de dâhil olmak üzere geliştirme ekibi tarafından yürütülecek tüm testler;
2. Tamamlamayı onaylayacak onaylayıcıların belirlenmesi;
3. Güvenlik açığı değerlendirmeleri ve tehdit modellemesi gibi güvenlik testi gereklilikleri; ve
4. Test ortamı, yaklaşımı, süreci ve bir üst ortama aktarım yolu.

Proje ömrü boyunca sürüm hazırlık kriterleri, içerik ve teslimat sıklığı da dâhil olmak üzere TEST ve PROD ortamlarına sürüme ilişkin ön koşulları ve süreci özetleyen bir sürüm stratejisi hazırlanmalıdır.

Sözleşmede belirtildiği durumlarda, yazılım dağıtımları Citi onaylı araçlar ve iş akışları kullanılarak Citi onaylı bir formatta paketlenmelidir.

17.32 Test

Çözümün tanımlanan gereklilikleri ve başarı kriterlerini karşıladığını doğrulamak için test kontrollü bir ortamda planlanmalı ve yürütülmelidir. Test senaryoları gerekliliklere ve kod commitlerine kadar izlenebilir olmalıdır.

Tedarikçi, başarılı/başarısız sonuçları, geliştirme sırasında gerçekleştirilen ek testleri ve tamamlanmamış tüm testleri (nedenleriyle birlikte) özetleyen bir rapor (bir "Test Çıkış Raporu") hazırlamalıdır. Çözümlememiş sorunlara yönelik azaltma planlarının yanı sıra kusurlar ve ertelenen işlevler belgelenmelidir.

Citi'nin talebi üzerine Tedarikçi aşağıdakilerin kanıtını sağlamalıdır:

1. Ayrıntılı bir Test Planı;
2. Bir Test Çıkış Raporu kapsamında ayrıntıları verilen test tamamlanma durumu ve sonuçları; ve
3. Test sonuçlarının gerekliliklere ve kod commitlerine kadar izlenebilirliği.

17.33 Dağıtım

Dağıtım öncesinde Tedarikçi, güvenlik açığı taramaları ve tehdit modelleme de dâhil olmak üzere gerekli tüm güvenlik testlerini tamamlamalıdır. Sürüm yayımlama süreci, belgelenmiş değişiklik kayıtları, geri alma stratejileri ve gerekli onaylarla yapılandırılmalıdır. Uygulama planları ve dağıtım rehberleri izleme ve eskalasyon protokollerini içermelidir.

Dağıtımın ardından Tedarikçi, denetime hazır olmayı sağlamak için sistem tanımlayıcılarını kesinleştirmeli ve ilgili tüm artefaktları güncellemelidir.

17.34 Güvenlik

1. Kod yazılmadan önce potansiyel güvenlik risklerini, zafiyetleri ve mimari zayıflıkları belirlemek ve ele almak amacıyla SDLC'nin tasarım aşamasında yürütülen yapılandırılmış bir değerlendirme (bir "Güvenlik Tasarım İncelemesi"), OWASP gibi sektör standartlarıyla uyumlu önleyici ve tespit edici kontrollerle birlikte SDLC'ye dâhil edilmelidir.
2. Güvenli kodlama uygulamaları uygulanmalıdır.
3. Tedarikçi bilgi güvenliği kontrollerini, uygulamaların, ürünlerin ve hizmetlerin seçimi, geliştirilmesi ve uygulanması için kendi süreçlerine ve prosedürlerine dâhil etmelidir.
4. Tedarikçi, Citi Bilgilerinin saklandığı, işlendiği ve/veya iletiildiği tüm sistemler için güvenli bir kurulum prosedürüne sahip olmalı ve tüm sistemler için güvenli bir imaj veya şablon sürdürmelidir.

17.35 Kötü Amaçlı Yazılımlara Karşı Kontroller

Tedarikçi, herhangi bir kötü amaçlı kodun (ör., virüsler, solucanlar, Truva atı virüsleri, reklam yazılımları, casus yazılımlar, fidye yazılımları veya verilerin tehlikeye düşebileceği diğer benzer siber saldırılar) girişini önlemek ve tespit etmek için kontrollerin uygulanmasını sağlamalıdır. Tedarikçi şunları yapmalıdır:

1. Tüm kişisel bilgisayarlarda virüs önleme ve casus yazılım önleme teknolojisini ve Citi verilerini saklayan, işleme alan ve/veya ileten tüm Yerel Alan Ağı (LAN) sunucularında, posta sunucularında ve diğer cihazlarda teknolojiyi uygulamalı, güncellemeli ve idame etmelidir.
2. Kullanıcıların antivirüs/kötü amaçlı yazılımı önleme araçlarını ve planlı taramaları devre dışı bırakmalarını önleyecek güvenlik ayarları kullanılmalıdır.
3. Antivirüs ve kötü amaçlı yazılımı önleme yazılımlarını yapılandırmaya ve güncellemeye yönelik merkezî olarak yönetilen, otomatik prosedürlere sahip olmalıdır.
4. Antivirüs imzaların veya tarama motorlarının eski olduğu uyumlu olmayan bilgisayarları tanımlamak ve ele almak için süreçler uygulanmasını sağlayın.
5. Depolama medyası dâhil ancak bununla sınırlı olmamak üzere hariç cihazlara bağlantıya izin veren iletişim bağlantı noktalarına/arayüzlerine erişimi kontrol edin.

17.36 Mobil Koda Karşı Kontroller

Tedarikçiler, güvenli mobil kod uygulamaları etrafında kontrollerin uygulanmasını sağlamalıdır. Mobil kod kullanımına izin verildiğinde yapılandırma, en azından ilgili tüm endüstri standartlarını ve Citi'ye karşı sözleşmeden doğan yükümlülükleri karşılamalıdır. Tedarikçi, izin verilen mobil kodun açıkça tanımlanmış ve belgelenmiş bir güvenlik politikasına göre çalışmasını sağlamalı ve yetkisiz mobil kodun çalışmasını önlemelidir.

Temel işletim sistemini veya platformu etkileyebilecek (yani “korumalı alan”ın dışında) mobil kod için Tedarikçi aşağıdakileri sağlamalıdır:

1. Tedarikçi tarafından yayımlanan mobil kod, Citi onaylı bir Sertifika Yetkilisi tarafından imzalanmalı; sertifikanın yaşam döngüsü, sertifikanın süresinin dolması veya rotasyonu hususlarını ele alacak şekilde Tedarikçi tarafından yönetilmelidir.
2. Süresi dolmuş sertifikalara sahip imzalı mobil kodun üretimden kaldırılması gerekir.

17.37 Denetim Günlüğü

Tedarikçi, Citi verilerine erişmek, saklamak, işleme almak, yönetmek ve/veya iletmek için kullanılan tüm Kontrollü Bilgi Sistemlerinin aşağıdaki ögeleri kaydetmek üzere bir altyapı veya uygulama düzeyinde denetim izlerini sürdürmesini sağlamalıdır:

1. İlişkili platform için altyapı güvenliğiyle ilgili eylemler.
2. Bir güvenlik duvarı veya IDS/IPS tarafından oluşturulan güvenlik olayı ile ilişkili tüm sistem alarmları
3. Tüm girişilen sistem güvenliği ihlalleri (ör., başarısız Kullanıcı oturum açma denemeleri)
4. Kaynaklara (yazılım, veri, süreçler, vb.) yetkisiz erişim denemeleri
5. Yönetici eylemleri
6. Bir kullanıcıdan veya başka bir sistemden belirli bilgilerin alınmasıyla ilgili bilgiler
7. Özellikle aşağıdaki ögeleri içeren finansal işlemler ve Citi Bilgileri ile ilgili tüm önemli olaylar:
 - a. Finansal işlemlere ilişkin güncellemeler
 - b. Gizli veya Hassas PII veri güncellemeleri
 - c. Kısıtlanmış verilerle ilgili güncellemeler
 - d. Kimlik Doğrulama verilerinde güncellemeler
8. Oluşturulan tüm oturumlar
9. Benzersiz cihaz kimliği gibi oturum artefaktları, teknik olarak mümkün olduğunda yakalanmalı ve dolandırıcılık soruşturmalarını desteklemek üzere Citi'ye dönük uygulamalar (ör., web siteleri ve mobil uygulamalar) için günlüğe kaydedilmelidir. Bu artefaktlar en azından IP adreslerini içermelidir. Bu artefaktlar Citi işlemleri ve Citi hesabı açma faaliyetleri için yakalanmalıdır. Oturum artefaktının işlemle veya hesap açma işlemiyle ilişkilendirilebilmesi için gerekli bilgiler yakalanmalıdır.
10. Denetim izleri, reddedilmeyi önlemek için belirli bir aktivitenin belirli bir kişiye atfedildiğini belgelemelidir.
11. Önemli Bilgi Güvenliği Yönetimi (ISA) olayları, aşağıdaki ögeler de dâhil olmak üzere özel olarak günlüğe kaydedilmelidir:
 - a) Kullanıcı oluşturma
 - b) Kullanıcı erişim haklarının değişikliği
 - c) Kontrollü Bilgi Sisteminde profillerin silinmesi, oluşturulması ve değiştirilmesi
 - d) Şifre sıfırlamaları
 - e) Sistem güvenlik yapılandırmasındaki değişiklikler

- f) Ayrıcalıklı İşlevsel Kimliklerin tüm etkileşimli etkinlikleri
- g) Güvenlik günlükleri, söz konusu bilgilerin eklenmesinin teknik olarak mümkün olmadığı durumlar dışında, günlüğü oluşturan sistemden bağımsız olarak en az aşağıdaki bilgileri içermelidir:
 - I. Olayın tarihi ve saati (UTC formatlı saat)
 - II. İşlemi gerçekleştiren kişinin kullanıcı kimliği
 - III. Olay türü
 - IV. Etkilenen varlık veya kaynak adı
 - V. Erişim türü (silme, değiştirme vb.)
 - VI. Olayın başarılı veya başarısız olması
 - VII. Kaynak (terminal, port, konum, IP, Ana Bilgisayar Adı, vb.)

17.38 Günlük Bilgilerinin Korunması

Tedarikçi, başlatma, kapatma, depolama ve iletim sırasında denetim izlerinin bütünlüğünü korumak için erişim kontrollerinin uygulanmasını sağlamalıdır.

1. Denetim günlüklerine yetkisiz değişiklikleri önlemek için, Tedarikçi günlüklerin üzerine yazılamamasını veya etkinliğini izledikleri sistem kullanıcıları tarafından değiştirilememelerini sağlamalıdır.
2. Tedarikçi, Citi'ye günlük verileri için verilerin nasıl muhafaza edildiğini tanımlayan ve yürürlükteki tüm yasal ve düzenleyici gerekliliklere atıfta bulunan uyum önlemlerini içeren bir kayıt saklama prosedürü sunmalıdır.
3. Bir organizasyon veya güvenlik etki alanı içindeki tüm ilgili bilgi işleme sistemlerinin saatleri doğru bir zaman kaynağı ile eşitlenmelidir.

17.39 İzleme Sisteminin Kullanımı

Tedarikçiler, aşağıdaki olayların yakalanmasını, kaydedilmesini ve doğrudan veya otomatik bir inceleme süreci yoluyla gözden geçirilmesini sağlamalıdır:

1. Güvenlik duvarı veya Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tarafından oluşturulan bir güvenlik olayıyla ilişkili tüm sistem alarmları.
2. Güvenli standart yapıda tanımlandığı şekilde kritik kaynaklara yönelik tüm güncellemeler.
3. Gizli PII veya daha üst düzeyde sınıflandırılmış bilgilere erişimi olan herhangi bir kimlik (işlevsel, ayrıcalıklı, sistem, geçici, vb.) tarafından gerçekleştirilen tüm etkileşimli etkinlikler.
4. Aşağıdaki istisna dışında yukarıdaki Denetim günlüğü bölümünde listelenen Önemli ISA Olayları:
 - a) Bilgi Güvenliği İdare etkinliğinin uçtan uca bütünlük kontrollerine sahip otomatik bir iş akışı/karşılama sistemi tarafından yürütüldüğü durumlarda kullanıcı, rol veya profilden yetkilerin kaldırılması.

17.40 Günlük Bağıntısı ve İncelemesi

1. Günlüğe kaydedilen bir olay bir uyarıyı tetiklediğinde ve olay incelendiğinde, potansiyel olarak zararlı bir bilgi güvenliği olayının meydana gelmiş olabileceğine dair bir belirti varsa, Tedarikçi takip işlemleri başlatmalı ve bir soruşturma yürütmelidir.

2. Tedarikçi, denetim günlüklerinin bir Güvenlik Bilgileri ve Olay Yönetimi (SIEM) sistemi veya günlük bağıntısı analizi ve incelemesi için günlük analizi aracı gibi merkezî bir günlük yönetim sisteminde toplanmasını sağlamalıdır.
3. Tedarikçiler, işlem yapılabilir olayların tanımlanmasını iyileştirmek için SIEM veya günlük analizi araçlarının yapılandırmasını periyodik olarak incelemeli ve ayarlamalıdır.

17.41 Operasyon Yazılımının Kontrolü

Tedarikçi, yalnızca sektör tarafından kabul gören bir ticari sağlayıcı tarafından desteklenen veya güvenlik sorunlarını ele almaya yönelik olarak aktif ve uygun şekilde yamalar yayınlayan ve yapılandırma güncellemeleri yapan işletim sistemlerinin ve yazılımların kullanılmasını sağlamalıdır.

Tedarikçi, onaylanmış tüm güvenlik yamalarının ve yapılandırmaların uygulanacağı düzeltme sürelerini belirten, belgelenmiş bir sürecin uygulanmasını sağlamalıdır.

Tedarikçi ile Citi arasında ayrı bir bakım sözleşmesinden bağımsız olarak, Tedarikçi, Citi için geliştirilen ve bir lisans anlaşması altında yönetilen yazılımın, bilinen güvenlik açıkları olan desteklenmeyen yazılım sürümlerinin kullanımına izin verilmemesini ve bu yazılımın zamanında gereken şekilde güncellenmesini ve yamalanmasını sağlamalıdır.

Citi Bilgilerini işlemek için kullanılan uygulama yazılımı, yerleşik Tedarikçilerden alınmalı ve lisanslanmalı, kataloglanmalı ve desteklenmelidir.

17.42 Güvenlik Açığı ve Tehdit Yönetimi

1. Tedarikçi, aşağıdakilerin tümünü kapsamlı bir şekilde ele alan ve/veya içeren bir güvenlik açığı ve tehdit yönetimi süreci uygulamalıdır:
 - a. Citi'ye ait Gizli veya daha hassas verileri işlemek, saklamak, bunlara erişmek ya da bunları iletmek için kullanılabilecek tüm varlıklardaki güvenlik açıklarını keşfetmeye ve yönetmeye yönelik araçlar ve prosedürler.
 - b. Sektörce tanınan güvenlik açığı araçları ve raporlama metodolojisi kullanılarak taramaların en az haftalık olarak gerçekleştirilmesi gerekliliği.
 - c. Güvenlik açıklarının, en güncel "Common Vulnerability Scoring System (CVSS)" sürümüne (bkz. <https://www.first.org/cvss>) göre sıralanması ve önem derecesine dayalı düzeltme sürelerinin belirlenmesi.
 - d. Tam üretim yerleştirmesinden önce güvenlik açığı düzeltmelerinin test edilmesi gerekliliği.
 - e. Kritik güvenlik açıklarının iyileştirilmesini hızlandırmaya yönelik belgelenmiş ve tekrarlanabilir bir operasyonel süreç.
 - f. Tedarikçi, Kullanım Ömrü Sonu (EOL) veya Satıcı Desteği Sonu (EOVS) durumlarına hazırlanmak amacıyla varlıkları desteklenebilir kullanım ömürleri boyunca takip etmeli ve bu tür varlıkları proaktif olarak yükseltmek veya değiştirmek için yürürlükte süreçlere sahip olmalıdır.
 - g. İstihbarat toplama, güvenlik açığı taramaları veya sızma testleri yoluyla belirlenen tüm kritik CVSS puanlama güvenlik açıklarına öncelik verilmeli

ve güvenlik açığı riskiyle orantılı, iyi tanımlanmış bir zaman dilimi içinde düzeltilmelidir.

17.43 Üçüncü Tarafça Barındırılan Uygulamalar

Tedarikçi, Citi Gizli veya daha hassas verilerini bir web sitesinde veya İnternette erişilebilen bir sistemde veya Citi markalı bir web sitesinde muhafaza eder veya saklarsa, Citi'yi etkileyen ürün veya hizmetleri içeren bir güvenlik açığına veya tehdide (her biri bir "güvenlik açığı") karşı koruma sağlamak için, Tedarikçi aşağıdaki gerekliliklerine uymalıdır.

1. Citi'nin bilgi güvenliğine ilişkin sorularına yanıt vermesi için bir Tedarikçi çalışanı atamalıdır.
2. FIRST, CERT/CC, CISA Known Exploited Vulnerabilities Catalog ve satıcı posta listeleri gibi saygın bilgisayar güvenliği açığı bilgi kaynaklarını en az haftada bir izlemek için sektörcü kabul görmüş en iyi uygulamalardan yararlanmalı ve ilgili hizmet paketlerini, yamaları, yükseltmeleri ve geçici çözümleri edinmek, kapsamlı biçimde test etmek, uygulamak ve Citi'ye sunmak için uygun önlemleri almalıdır.
3. Ağ, sistem ve uygulama güvenlik açığı tarama araçlarını ve/veya sızma testini kullanarak bilgi güvenliği önlemlerinin uygulanmasını en az üç ayda bir test etmelidir.
4. Politikaların, süreçlerin gözden geçirilmesi dâhil ancak bunlarla sınırlı olmamak üzere, Tedarikçinin herhangi bir sözleşme kapsamındaki yükümlülüklerine ve bu Gerekliliklere uygunluğunu doğrulamak için Citi'nin veya Citi onaylı bir üçüncü tarafın, makul sürelerde güvenlik açığı değerlendirmeleri, etik saldırılar veya diğer güvenlik değerlendirmelerini yapmasına ve bu denetimleri gerçekleştirmek için ticari olarak mevcut araçları ve/veya endüstri standardı uygulamaları kullanarak fiziksel güvenlik düzenlemelerinin yerinde değerlendirilmesi, ağ, sistem ve uygulama güvenlik açığı taraması ve sızma testi yapmasına izin vermelidir.
5. Tedarikçiye güvenlik açığı değerlendirme hizmetleri sağlayacak tüm yüklenicilerin Citi onaylı güvenlik açığı değerlendirme sağlayıcıları listesinde yer alması gerekir. Tedarikçi, Hizmetleri sağlamak için yüklenici veya alt yükleniciler kullandığında, gerekli tüm güvenlik açığı değerlendirmelerinin, Hizmetleri doğrudan kendisi sağlıyormuşçasına aynı süreler içinde ve masrafları kendisine ait olmak üzere tamamlanmasını sağlamalıdır. Ayrıca, herhangi bir yüklenici veya alt yüklenicinin bu tür değerlendirmeleri kolaylaştırma yükümlülüğünün, Citi'ye söz konusu değerlendirmeleri yapma yetkisi veren hükümler de dâhil olmak üzere, Tedarikçi ile yüklenici/alt yüklenici arasındaki Hizmetle ilgili sözleşmede yazılı hâle getirilmesini sağlamalıdır.
6. **Bildirim.**
 - a) Tedarikçi, Citi'yi etkileyen bir ürün veya hizmetle ilgili bir güvenlik açığı tespit ettiğinde, tespitten itibaren 24 saat içinde Citi'yi yazılı olarak bilgilendirmeli ve bildirimine Tedarikçinin uyguladığı düzeltici eylemlerin açıklamasını eklemelidir.

b) Tedarikçi, sorumlu kamusal açıklama kanalları aracılığıyla yapılan açıklamanın ardından (Güvenlik Açığının National Vulnerability Database (NVD) içinde yayımlanması veya haricî güvenlik satıcılarına sağlanan bir tehdit kataloğunda yer alması), Citi'yi etkileyen bir ürün ya da hizmetle ilgili güvenlik açığından haberdar olursa söz konusu yayından itibaren 24 saat içinde Citi'yi yazılı olarak bilgilendirecektir. Her bildirim; güvenlik açığı, sistemin Citi ile ilgili hizmetler bakımından kullanım amacı (yani Citi Bilgilerini barındırıp barındırmadığı, hizmetlerin sunumunda kullanılıp kullanılmadığı veya her ikisi), uzaktan istismar edilip edilemeyeceği ve Common Vulnerabilities and Exposures (CVE) puanı hakkında bilgi içerecektir. Tedarikçi, güvenlik açığı giderilene kadar Citi'ye güncellemeler sağlamaya devam edecektir. Citi'nin bir güvenlik açığı tespit ettiği durumlarda Citi, Tedarikçiyi bu konuda bilgilendirebilir ve Tedarikçi güvenlik açığını bu Maddeye uygun olarak derhâl giderecektir.

7. **İyileştirme.** Bu madde kapsamında bildirilen her Güvenlik Açığı için bildirimde bulunan taraf, söz konusu güvenlik açığının risk düzeyini ve etkisini önem derecesi ile Citi'ye yönelik riske göre değerlendirecek ve Ek A'da belirtildiği üzere Common Vulnerability Scoring System'a (CVSS) dayalı bir risk öncelik düzeyi atayacaktır (bkz. <https://www.first.org/cvss>). Bir risk seviyesi belirlenip taraflarca kabul edildikten sonra, Tedarikçi, tanımlanmış herhangi bir orta, yüksek veya kritik güvenlik açığını düzeltecektir. Mümkün olduğunda, bu güvenlik açığı düzeltilmesi, şu anda dağıtılan sürüme karşı bir güvenlik paketinde sunulmalıdır.

Tedarikçi, güvenlik açığını Citi'yi tatmin edecek şekilde gideremezse veya bu konuda isteksizse, Citi herhangi bir ek yükümlülük veya mali yükümlülük olmaksızın (sonlandırılan kısım için) geçerli lisansı feshedebilir ve Tedarikçi ödenen lisans ücretlerinin orantı kısmını derhâl Citi'ye iade edecektir.

17.44 İletişim Güvenliği Ağ Kontrolleri

1. Citi Bilgilerine erişmek, bunları saklamak, yönetmek, işlemek ve/veya iletmek için kullanılan Tedarikçi ağları tehditlere karşı korunmalı ve ağdaki kontrol noktaları kullanılarak Bilgi Sistemlerinin güvenliği sürdürülmelidir.

- a. Citi Bilgi Sınıflandırması Gizli veya daha yüksek olan bilgiler, İnternet'e açık Askerden Arındırılmış Bölgedeki (DMZ) bir sistemde kalıcı olarak saklanmamalıdır. Citi Bilgilerine Kablosuz Yerel Alan Ağları (WLAN'lar) veya yetkisiz erişimi engellemek için makul kontroller içeren diğer kablosuz cihaz çözümleri (PEAP-TLS, EAP-TTLS vb.) kullanarak Citi Bilgilerine erişmek, depolamak, yönetmek, işlemek ve/veya iletmek için kullanılan ağlar, Citi Bilgilerini içeren ağlara bağlanabilir.
 - b. Tedarikçinin küresel ağına yapılan tüm haricî IP bağlantıları, Tedarikçi tarafından yönetilen bir güvenlik duvarı tarafından korunmaktadır.
 - c. Citi bilgilerinin erişildiği, yönetildiği, saklandığı, işleme alındığı veya iletildiği Tedarikçinin ağlarına yönelik internet bağlantılarını izleyen ve koruyan gerçek zamanlı bir Saldırı Tespit Sistemi (IDS) ve Saldırı Önleme Sistemi (IPS) işletilmektedir.
2. Tüm Citi markalı İnternet uygulamaları için Tedarikçi şunları sağlamalıdır:
- a. Tedarikçi tesislerinde barındırılan hizmetler, Citi onaylı anti-DDoS (Distributed Denial of Service) hizmetleri veya Citi tarafından doğrulanmış karşılaştırılabilir kontrollerle korunmalıdır.
 - b. Haricî güvenlik duvarlarının varsayılan olarak reddetme kuralıyla yapılandırılması gerekir. Güvenlik duvarı kuralları en az ayrıcalık ilkesine göre yapılandırılmalı ve güvenlik duvarının reddettiği tüm bağlantı girişimleri (ör., bırakılan paketler) günlüğe kaydedilmeli/kayıt altına alınmalıdır.
 - c. Yönetilen arayüzlerde ağ iletişim trafiği varsayılan olarak reddedilmeli ve yalnızca istisna yoluyla izin verilmelidir. İstisnalar belirli kaynaklar, hedefler ve hizmetlerle çok sınırlı olmalıdır.
 - d. Web uygulaması trafiği uygun kontrollere sahip olmalı ve Web Uygulaması Güvenlik Duvarları gibi araçlar aracılığıyla filtrelenmelidir.

17.45 Ağlarda Ayrım

Tedarikçi, Citi Bilgilerine erişmek, bunları saklamak, işleme almak, yönetmek ve/veya iletmek için kullanılan ve İnternet yoluyla erişilebilen tüm Bilgi Sistemlerine ve uygulamalarına sadece Tedarikçinin kurum içi yerel ağdan tecrit edilmiş bölgesi (DMZ) yoluyla erişilmesini sağlamalıdır.

Acil bir olay sırasında Tedarikçi, ağ Güvenlik Olaylarının etkisini azaltmak için (örneğin, bir virüs salgını sırasında bağlantı noktası filtreleme) ağın bölümleri arasındaki erişimi filtreleyebilmelidir.

Uzaktan Erişim ve Ana Bilgisayar Güvenliği, Tedarikçi ağındaki ağ kaynaklarına erişimi sınırlamak için grup bazlı erişim kontrolleri (ör., personel, alt yükleniciler) uygulamalıdır. Ana bilgisayar düzeyinde, erişim kontrolü grup veya birey düzeyinde yapılabilir.

17.46 Ağlarda Ekipman Tanımlama

Teknoloji platformları, etkileşimin ve diğer hafifletici denetimlerin IS risk düzeyleriyle orantılı olarak eş teknoloji platformlarını tanımlamalı ve doğrulamalıdır.

1. Sadece gerekliliklere uyan ve Tedarikçinin yetkilendirdiği Tedarikçi cihazları (diğer deyişle, donanım dâhil, ancak bununla sınırlı olmamak kaydıyla, masaüstü ve dizüstü bilgisayarlar) Citi Bilgilerinin depolandığı, işlendiği veya

- aktarıldığı Tedarikçi Ağına erişebilir.
2. Yalnızca bu gerekliliklere uyan ve Citi tarafından yetkilendirilen Tedarikçi cihazları (donanım dâhil, ancak bununla sınırlı olmamak kaydıyla, masaüstü bilgisayarlar, dizüstü bilgisayarlar, çıkarılabilir veri saklama medyaları) Citi ağına erişebilir.

17.47 Güvenlik Gereklilikleri Analizi ve Spesifikasyonu

Tedarikçi bilgi güvenliği prosedürlerini, uygulamaların, ürünlerin ve hizmetlerin seçimi, geliştirilmesi ve uygulanması için kendi süreçlerine ve prosedürlerine dâhil etmelidir.

17.48 Çevrim İçi İşlemler

1. Uygun durumlarda, Tedarikçi kimlik bilgilerini doğrulamak için dinamik parolaları veya dijital sertifikaları kullanan Bilgi Sistemlerine sahip olmalıdır.
2. Tüm son kuruluş sertifikalarının en az 13 ayda bir değiştirilmesi gerekir.
3. Citi bilgilerini saklayan, işleyen, yöneten veya bunlara erişen, Citi markalı Internet'e dönük uygulamaları barındıran veya Citi'nin ağ kaynaklarına bağlantısı olan tüm Tedarikçi uygulamaları:
 - a. Erişilen veri/işlev türlerine dayalı bir kimlik doğrulama yöntemi kullanmalıdır;
 - b. Çok Ögeli Kimlik Doğrulama (MFA) uyumluluk değerlendirmesi yapmalı ve gerekirse önerileri uygulamalıdır;
 - c. Şüpheli Aktivite İzleme (SAM) kabul değerlendirmesi gerçekleştirmeli ve gerekirse önerileri uygulamalıdır;
 - d. Tüm bu durumlarda, Tedarikçi, Citi'nin mevcut gereklilikleri için birincil iş irtibatı ile iletişime geçmelidir.

17.49 Değişiklik Kontrol Prosedürleri

1. Tedarikçiler, güvenlik duvarlarına, Yetkisiz Giriş Tespit Sistemlerine (IDS) ve Yetkisiz Giriş Önleme Sistemlerine (IPS) yönelik yapılandırma değişikliklerinin Tedarikçi değişiklik yönetim süreci üzerinden yönlendirilmesini sağlamalıdır.
2. Geçici kimlikler yoluyla üretime verilen erişim kaydedilmeli ve ortama yönelik yapılan değişikliklerin izlenmesi için gözlemlenmelidir.
3. Citi sınıflandırması Gizli veya daha yüksek olan veya IS risk bileşeni değeri "Bütünlük" veya "Kullanılabilirlik" için "Yüksek" olan Müşteri Bilgilerini içeren Kontrollü Bilgi Sistemleri için, Bölüm 17.32'ye (Denetim günlüğü) göre yakalanan günlükler Tedarikçi tarafından gözden geçirilmelidir. Bu gözden geçirmeler, uygun bir risk tabanlı örnekleme metodolojisine dayalı olabilir.
4. Gözden geçirme, geçici imtiyazlı erişimin bir parçası olan değişikliklerin tasarlanan şekilde yapılmış olduğunu doğrulamalıdır.
5. Tedarikçi, inceleme sürecine ilişkin kanıtların saklanması da dâhil olmak üzere tüm değişiklikleri belgelemelidir.

17.50 Bilgi Sızıntısı

Tedarikçi, aşağıdakiler dâhil olmak üzere bilgi sızıntısını önleyen, belgelenmiş bir güvenli kodlama standardına sahip olmalıdır:

1. Ayrıntılı sistem bilgileri (ör., sunucu türü ve teknolojisi).
2. Dizin ağacı yapısını ve altta yatan veri tabanı türünü ortaya çıkaran yığın izleri ve istisna hataları.

17.51 Test Verileri

Citi tarafından Gizli veya daha yüksek olarak sınıflandırılan bilgiler; endüstri standartlarını karşılayan araç ve yöntemlerle kimlikten arındırılmadıkça, maskelenmedikçe ve/veya artık hassas olmayacak şekilde gizlenmedikçe, Tedarikçi tarafından yazılım uygulaması geliştirme ya da test ortamlarında veya Laboratuvarlarda kullanılamaz veya saklanamaz; aksi hâlde Tedarikçi, geliştirme veya test ortamlarında canlı üretim kontrolleri uygulamalıdır.

17.52 Sistem Kabulü

Tedarikçi ilgili endüstri standartlarını karşılayan yürürlükte belgelendirilmiş Proje Kapsamı Yönetimine ve Sistem Kabul süreçlerine sahip olmalıdır.

17.53 Bilgi Güvenliği Zayıflığının Bildirilmesi

Tedarikçi, Citi bilgi varlıklarının ihlaline yol açan uygulama ve altyapı güvenlik açıklarının **derhâl Citi'ye bildirilmesini** sağlayan bir Sürece sahip olmalıdır.

17.54 Güvenlik Olayı Sorumlulukları ve Prosedürleri

1. Bir SIRT, güvenlik olayının nasıl veya nerede meydana geldiğine ya da ihlale kimin neden olduğuna bakılmaksızın aşağıdakilerden herhangi birini ihlal eden bir güvenlik olayıdır:
 - Citi verilerinin Gizliliği, Bütünlüğü veya Kullanılabilirliği.
 - Citi'nin sözleşmeden doğan, yasal veya regülasyonel yükümlülöklere tabi olduğu herhangi bir verinin (Kişisel Bilgiler dâhil) Gizliliği, Bütünlüğü veya Kullanılabilirliği.
 - Herhangi bir Citi verisini saklayan, işleyen veya ileten Citi bilgi sistemlerinin Bütünlüğü veya Kullanılabilirliği.
2. Amaçlarımız doğrultusunda gizliliğin ihlali, verilerin yetkisiz bir kişiye ifşa edilmesini veya Citi'nin veri üzerindeki gözetim ve kontrolünü kaybettiği senaryoları ifade eder. Tüm güvenlik olaylarının derhâl bildirilmesi gerekir.
3. Tedarikçi bir SIRT olayı yaşamışsa; Citi'nin kendi olay müdahale süreçleri uyarınca talep ettiği bilgileri sağlama, ihlal edilen verileri Citi'nin yasal, düzenleyici ve/veya dâhilî yönetim gerekliliklerini karşılamasına yetecek şekilde analiz etme konusunda Citi ile iş birliği yapmalıdır; kanun, kural veya düzenleme uyarınca gerekli olan ya da Citi'nin takdirine bağlı olarak istediği tüm bildirimleri Citi'nin talebi üzerine, masrafları Tedarikçiye ait olmak kaydıyla ve yalnızca Citi önerilen bildirim şablonu metnini inceleme ve değiştirme fırsatına sahip olduktan sonra yapmalıdır ve Citi özel olarak yazılı olarak adının geçmesini talep etmediği sürece Tedarikçi bu tür bildirimlerin hiçbirinde Citi'nin adını belirtmemelidir.

17.55 Veri Sızıntısı Koruması (DLP)

Tedarikçi, Citi Gizli veya daha yüksek gizlilik derecesine sahip verilere erişime sahip olan tüm personeli kapsayan içerik ve uç nokta izleme dâhil olmak üzere veri sızıntısı önleme (DLP) denetimleri uygulamalıdır.

Tedarikçi, Citi Gizli veya daha yüksek gizlilik derecesine sahip verilerin aşağıdaki kanallar üzerinden ağlarının dışına taşınmakta olduğu durumları tespit etmek ve önlemek için denetimlere sahip olmalıdır:

- a. Şifrelenmemiş e-postalar
- b. Şifrelenmiş e-posta ekleri
- c. Citi verilerinin yazdırılması
- d. Citi verilerinin ağları dışındaki konumlara aktarılması (ör., FTP üzerinden)
- e. Citi Gizli veya daha yüksek gizlilik derecesine sahip verileri USB sürücüler, çıkarılabilir sabit sürücüler, CD/DVD sürücüler ve veri depolama özelliğine sahip diğer çıkarılabilir cihazlar gibi çıkarılabilir medyaya kopyalama girişimleri. Bu ayrıcalık varsayılan olarak engellenmelidir.
- f. DLP çözümü, Citi Gizli veya daha yüksek gizlilik derecesine sahip verileri ağlarından diğer hedeflere taşıma, aktarma veya kopyalama girişimleri ortaya koyan (başarılı olmuş veya engellenmiş) tüm olayları günlüğe kaydetmeli ve Tedarikçiye bildirmelidir. Bu ayrıcalık varsayılan olarak engellenmelidir.
- g. Citi verilerinin SaaS/dosya paylaşım siteleri de dâhil olmak üzere haricî web sitelerine yüklenmesi. Bu ayrıcalık varsayılan olarak engellenmelidir.

17.56 Web'de Gezinme

1. Tedarikçi, Citi Gizli veya daha yüksek gizlilik derecesine sahip bilgilerin paylaşılmasını ve Citi verilerine erişime sahip çalışanların kötü amaçlı yazılım veya saldırılara maruz kalmasını önlemek için web erişimi denetimlerine sahip olmalıdır.
2. Citi Gizli veya daha yüksek gizlilik derecesine sahip verilere erişime sahip olan Tedarikçiler için:
 - a. Tüm URL talepleri günlüğe kaydedilmelidir.
 - b. Citi verilerinin yetkisiz paylaşımı için kullanılabilecek sitelere (web postası, sohbet, sosyal medya, çevrimiçi depolama, Gen-AI, vb.) erişim girişimleri engellenmelidir.
 - c. Ortamı kötü amaçlı yazılım veya saldırıya maruz bırakabilecek sitelere erişim engellenmelidir.
 - d. İşle ilgili olmadığı kabul edilen sitelere erişim girişimleri engellenmelidir.
 - e. Tedarikçi, düzenli olarak güncellenen bir URL sınıflandırma hizmetine abone olmalıdır; sınıflandırılmamış tüm URL'ler varsayılan olarak engellenmeli veya tüm URL'ler varsayılan olarak engellenip her bir durum için ayrı ayrı onaylanmalıdır.

- f. Tedarikçi tarafından kullanılan Web Tarayıcıları tam olarak desteklenir ve yazılım satıcısı tarafından sunulan en son güvenlik güncellemeleriyle güncel tutulmalıdır.

17.57 Elektronik Mesajlaşma

Anlık mesajlaşma, eşler arası ağlar veya diğer İnternet iş birliğine dayalı araçlar, Bölüm 17.9 (kriptografik kontrollerin kullanımı konulu Politika) uyarınca tüm Citi verileri için yürürlükte uygun bir şifreleme olmadıkça, Tedarikçi ağı dışına veya Citi Bilgilerini içeren ağlardan Citi Bilgilerini iletmek veya saklamak için kullanılamaz.

17.58 E-posta

Tedarikçi, Citi bilgilerinin paylaşılmasını ve kötü amaçlı yazılım veya saldırılara maruz kalmasını önlemek için e-posta denetimlerine sahip olmalıdır. Şunları içerir:

1. E-posta geçidine giren gelen dosya ekleri taranır ve sistem için bir risk teşkil ederlerse engellenirler.
2. E-posta filtreleme (İstenmeyen Posta Önleme, Kimlik Avı Önleme) yazılımı kullanımdadır ve günceldir.
3. Citi Gizli veya daha yüksek gizlilik seviyesine sahip veriler Tedarikçinin kuruluşu dışına gönderildiğinde şifrlenmelidir.
4. Tedarikçi tarafından kullanılan e-posta istemcileri tam olarak desteklenir ve yazılım satıcısı tarafından sunulan en son güvenlik güncellemeleriyle güncel tutulur.

17.59 Çıkarılabilir Medya

1. Tedarikçi, Citi Bilgilerini, hangi medyada tutulursa tutulsun korumakla yükümlüdür. Bu standart, bilgilerin saklandığı aşağıdaki türdeki medyalar için geçerlidir ancak bunlarla sınırlı değildir: kart, kaset, kompakt disk (CD), çek kâğıdı, disket veya diğer çıkarılabilir depolama cihazı, basılı çıktı, manyetik disk, manyetik bant, mikrofilm, mikrofiş, optik disk veya kâğıt belge.
2. Citi Bilgilerinin saklandığı sistemlerde taşınabilir medya/depolama cihazlarına erişim için varsayılan ayar, erişim olmamasıdır. İstisnalar tanınıp okuma-yazma erişimine izin verilmesi durumunda, taşınabilir medya cihazında verilerin şifrlenmesi gerekir.
3. Çıkarılabilir medya kullanımına izin verilirse, söz konusu kullanım için çıkarılabilir medyanın kullanımını gerekli kılan iş gerekçesi dâhil olmak üzere bir yönetim onayı süreci olmalıdır. Çıkarılabilir medya yönetim tarafından envantere kaydedilmelidir. Citi Gizli veya daha yüksek gizlilik seviyesine sahip verileri içeren çıkarılabilir medya, kullanıcı tarafından yapılması gereken bir işlem olmaksızın otomatik olarak şifrlenmelidir.

17.60 Medya İmhası

1. Gizli veya daha üst düzey bir Citi Bilgi sınıflandırmasına sahip Citi Bilgilerinin Citi tarafından verilen talimatlar doğrultusunda imhası uygun olduğunda (diğer deyişle, bilgilerin artık Citi için gerekli veya kullanışlı olmadığı noktada, ayrıca kanun, regülasyon ve/veya Citi politikalarına göre ek bir tutma zorunluluğunun süresi dolduğunda), Tedarikçi bu tür bilgileri kullanılamayacak ve geri kurtarılamayacak şekilde imha etmelidir.

2. Takılabilir medyaları aşağıdaki kurallara göre güvenli biçimde silmek için, sürücü sektörlerinin üzerine belirli ve farklı karakterleri rastgele yazan onaylı bir araç kullanılmalıdır:
 - a. Gizli veya daha yüksek gizlilik derecesine sahip olarak sınıflandırılan bilgileri depolayan medya için, söz konusu araç medyanın üç geçişini tamamlamalıdır.
 - b. Medyanın manyetikliğini giderin (varsa).
3. Medyayı okunamaz duruma getirmek için fiziksel olarak imha edin (ör., kırma, sürücüleri ezme).
4. Gizli veya daha yüksek gizlilik derecesine sahip Bilgiler içeren kâğıt ve diğer elektronik olmayan depolama medyaları, nihai imhadan önce güvenli bir şekilde toplanmalı ve güvenli bir "Gizli Kutu"da saklanmalıdır. Gizli Belge Kutuları her zaman kilitli olmalı ve yalnızca yetkili personel tarafından açılabilir.
- a. Citi Gizli veya daha yüksek gizlilik derecesine sahip bilgiler içerebilecek olan Fotokopi Makineleri, Yazıcılar, Faks Makineleri ve belleği/depolama alanı olan diğer cihazlar da temizlenmelidir.

17.61 Bilgi Güvenliği Yönetimi ve Eğitimi

1. Kimlik avı ve diğer sosyal mühendislik saldırılarının önlenmesini, Gizli veya daha yüksek sınıflandırılmış bilgilerin uygun şekilde işlenmesini ve güvenlik olaylarının bildirilmesi ile müdahale yönetimini içeren ancak bunlarla sınırlı olmayan uygun bir siber/bilgi güvenliği farkındalık ve eğitim programını sürdürmek.
2. Tedarikçi, yükleniciler ve geçici personel dâhil olmak üzere tüm çalışanların uygun farkındalık eğitimini ve iş görevlerine uygun şekilde kurumsal politika ve prosedürlere ilişkin eğitimleri almalarını sağlamalıdır.
3. Tedarikçi, eğitim ve farkındalık programının siber güvenlik ortamında ortaya çıkan riskleri ve tehditleri, mevcut en iyi uygulamaları ve yeni teknolojileri ele almak için yıllık olarak incelenmesini ve güncellenmesini sağlamalıdır.
4. Asgari olarak, aşağıdaki konular dâhil edilmelidir:
 - b. Bilgi etiketleme ve işleme
 - c. Güvenli İletim (güvenli e-posta, güvenli SharePoint depolaması, Citi'nin sahibi olduğu verileri kişisel e-postalara göndermemek)
 - d. Bilgi güvenliği olaylarının bildirilmesi
 - e. Güvenli iş yeri (ör., uygun internet kullanımı, yetkisiz yazılım, onaylanmamış yazılım indirme yasakları)
 - f. Parola Yönetimi (ör., güçlü parolalar, parola paylaşım yasağı)
 - g. Sosyal Mühendislik (ör., kimlik avı, hedefli kimlik avı, kişisel bilgilerin telefonla ele geçirilmesi, SMishing)
 - h. Uzaktan Çalışma (ör., Güvenli/Emniyetli Bağlantı, Kişisel Cihaz Güvenliği)

5. Tedarikçi çalışanlarına, Citi verilerini barındıran sistemlere erişim sağlamadan önce veya bu erişim sırasında eğitim atanmalı ve eğitim, atama bildiriminde belirtilen son tarihe kadar tamamlanmalıdır.
 - a. Yasalarca yasaklanmadığı durumlarda, tüm personele yılda en az bir kez IS eğitimi verilmelidir.
6. Eğitim, yerel yasaların izin verdiği durumda, etkililiğinin ölçüsünü kaydetmeye yönelik bir artefakt içermelidir (ör., tamamlandıktan sonra başarılı/başarısız eşliğini içeren bir sınav).

17.62 Siber Risk Yönetim Programı

Tedarikçi ayrıca, asgari olarak aşağıdakileri içeren uygun bir siber risk yönetimi programını asgari olarak sürdürmelidir:

1. İyi tanımlanmış, belgelenmiş Bilgi Güvenliği Risk Yönetimi programı ve/veya açıkça tanımlanmış bir siber/bilgi risk yönetimi bileşenine sahip olan, Tedarikçinin siber risk iştahını tanımlayan ve siber kalıntı riskinin bu iştah ile uyumlu olmasını sağlayan bir operasyonel risk yönetimi programının idamesi.
2. Kuruluş içindeki genel güvenlik durumunu değerlendiren güvenlik denetimleri ve incelemelerinin toplanmasını ve/veya gerçekleştirilmesini içeren ancak bunlarla sınırlı olmayan sağlam bir güvenlik riski yönetimi yönetim programını sürdürmek ve Tedarikçinin siber risk iştahının aşılmadığının incelenmesi ve güvence altına alınması amacıyla en az yılda bir kez üst yönetime rapor vermek.
3. Tedarikçinin kredi/banka kartı işlemlerini, ödemelerini ve/veya bilgilerini işlediği, sakladığı ve/veya ilettiği durumlarda Tedarikçi için geçerli olan PCI Data Security Standards (PCI-DSS) ile uyumu sürdürmek.
4. Tedarikçinin teşebbüs edilmiş, şüphelenilen ve/veya fiilen gerçekleşmiş herhangi bir siber güvenlik olayını tespit etmek, sınırlandırmak, soruşturmak, olaya müdahale etmek ve olaydan kurtulmak için yeterli kapasiteye sahip olmasını sağlamak üzere endüstri standartlarıyla uyumlu bir kriz yönetimi planı ve uygulama kılavuzu ile bir Güvenlik Olayı Müdahale Ekibi planını sürdürmek.

17.63 Uygulama, API, Kod, Sistem ve Altyapı Güvenliği

Tedarikçinin yazılım uygulaması/uygulamaları barındırdığı, geliştirdiği, birlikte geliştirdiği, geliştirme ortamları sağladığı ve/veya tedarik ettiği durumlarda Tedarikçi; güvenlik kusurlarını belirlemek ve yetkisiz erişimi, değişikliği ve/veya kötü amaçlı yazılım ya da diğer kötü amaçlı kod biçimlerinin eklenmesini önlemek için söz konusu yazılım ve/veya yazılım yamaları üzerinde kod incelemeleri gerçekleştirecektir. Ayrıca uygulamanın (API'ler dâhil), temelindeki sistem hizmetleri, işletim sistemleri ve ağlarla birlikte; güvenlik olayı, gizlilik ihlali, dolandırıcılık, Gizli Bilgilere yetkisiz erişim ve/veya bunların ifşası, uygulamanın işlediği, sakladığı ya da ilettiği bilgilerin bütünlüğünün kaybı ve/veya Tedarikçinin Citi'ye sunduğu ürünlerin ve/veya hizmetlerin kalitesini etkileyebilecek kullanılabilirlik kaybıyla sonuçlanabilecek bilinen güvenlik açıkları ve kusurlardan arınmış olmasını sağlamak üzere güvenlik açığı testleri yapacaktır.

17.64 Mobil Güvenlik

Tedarikçinin mobil uygulama çözümü sağladığı durumlarda Tedarikçi aşağıdaki gerekliliklere uymalıdır:

1. Mobil uygulama yalnızca genel kullanıma açık (GA) / kararlı ve Google Android (Android Go hariç) ve/veya Apple iOS / iPadOS platformlarının EOL² olmayan sürümünü desteklemelidir. Mobil çözüm ek işletim sistemleri/versiyonları için destekle donatılmışsa, desteklenen işletim sistemleri/versiyonları Citi tarafından yapılandırılabilir
2. Mobil çözüm, bu belgenin 17.9 (Şifreleme Gereklilikleri) Bölümünde belirtilen şifreleme dâhil ancak bununla sınırlı olmamak üzere, şifreleme algoritmalarını desteklemek için normal talimat setleriyle donatılmayan mobil platformları/cihazları desteklememelidir.
3. Beta, erken erişim ve özellik önizleme sürümleri/sürümleri dâhil ancak bunlarla sınırlı olmamak üzere üretim öncesi işletim sistemi sürümlerine üretim ortamında izin verilmez.
4. Tedarikçi, mobil çözüm tarafından paketlenen/kullanılan ücretsiz ve açık kaynak yazılım kitaplıkları dâhil ancak bunlarla sınırlı olmamak üzere entegre üçüncü taraf bileşenlerinin bir listesini sunabilmelidir.
5. Mobil uygulama, mobil uygulamaların Apple App Store veya Google Play Store gibi halka açık uygulama mağazaları aracılığıyla yayınlanmasını sağlayan gerekliliklere ve en iyi uygulamalara uygun olmalıdır. Mobil uygulamanın dağıtımı/yayınlanması için öncelikli ve tercih edilen yöntem, listelenen genel uygulama mağazaları olacaktır.
6. Android mobil uygulamaları APK imza şeması v2+'dan yararlanmalıdır. APK İmza şeması sürüm 1 (diğer adıyla JAR imzalama) kullanılmamalıdır.
7. Mobil uygulama imzalama anahtarının türü ve uzunluğu, bu belgenin 17.9. maddesinde yer alan Şifreleme **Gereklilikleri** hükümlerine uygun olmalıdır.
8. Her uygulama imzalama anahtarı ve ilgili X.509v3 sertifikası ayrı ayrı yönetilmeli ve tek bir Uygulama Kimliğine/Paket Kimliğine atanmalıdır. İmzalama anahtarları uygulamalar arasında paylaşılmamalıdır.
9. Bir mobil uygulamanın, mobil cihazdaki verilerin saklanması gerektirmesi durumunda, cihazda yalnızca uygulamanın/hizmetin amaçları için gerekli olan veya yasal veya mevzuat gereklilikleri uyarınca gerekli olduğu sürece en güncel verileri saklamalıdır.
 - a. Kullanıcı verilerinin toplanması, işlenmesi ve/veya saklanması; General Data Protection Regulation (GDPR), 2002/58/EC (ePrivacy) Directive veya bunların bölgesel eş değerleri gibi gizlilik regülasyonları

² Platform sahibinden veya Tedarikçiden aktif olarak desteklenen ve düzenli güvenlik ve bakım güncellemeleri alan ürün sürümleri.

- dâhil ancak bunlarla sınırlı olmamak üzere yerel yasalara uygun olmalıdır.
- b. Entegre üçüncü taraf bileşenler (ör., kitaplıklar) kullanıcı verilerini toplamamalı, işlememeli ve/veya saklamamalıdır.
10. Mobil uygulamalar, hiçbir uygulama verisini herkesin erişimine açık hâle getirmemelidir.
- a. Verilerin diğer uygulamalarla paylaşılması gerekiyorsa, uygulamalar, söz konusu veri paylaşımının uygun şekilde gerekçelendirildiği ve belgelendiği asgari sayıda diğer uygulamayla yalnızca gerekli miktarda veriyi paylaşmak için ilgili işletim sistemlerine yönelik ticari açıdan makul teknikler, yöntemler ve kontrollerden yararlanmalıdır.
11. Mobil uygulamalar yalnızca ilgili mobil işletim sistemleri tarafından sağlanan güvenli iletişim olanaklarına dayanmalıdır. Örneğin,
- a. Android uygulamaları, uygulama bildiriminde ve/veya ağ yapılandırma dosyasında, herhangi bir ağ etki alanına yönelik güvenli olmayan ağ trafiğine izin verilmediğini açıkça beyan etmelidir.
- b. iOS/iPadOS uygulamalarının hiçbir istisna olmaksızın Uygulama Aktarım Güvenliğinden (ATS) yararlanması gerekir.
12. Kriptografik materyaller donanım destekli güvenli bir anahtar deposuna bağlanmalıdır.
13. Mobil uygulamalar yayın modunda oluşturulmalı ve şunları içermemelidir:
- a. Güvenlik kontrollerini atlayabilecek herhangi bir özellik veya yöntem,
- b. Tersine mühendisliği kolaylaştırma potansiyeline sahip kaynak kod dosyası adları, değişken adları, sembol adları, yorumlar vb. hata ayıklama bilgileri.
14. Mobil uygulamalar, uygulamanın çalışma zamanındaki davranışını değiştirebilecek veya izleyebilecek kötü amaçlı kodların enjeksiyonunu önlemek için etkili anti-hook veya kurcalama önleyici mekanizmalarla donatılmalıdır.
15. Mobil uygulamalar, tersine mühendislik saldırılarını engellemek için kapsamlı hata ayıklama önleme veya tersine mühendislik önleme/şaşırtma teknikleri uygulamalıdır.
16. Mobil uygulama paketleri, içeriklerinin özgünlüğünü ve bütünlüğünü doğrulamaya olanak tanıyan bir özellik ile donatılmalıdır (ör., kriptografik sağlama toplamı ve/veya dijital imza kullanılarak).
17. Mobil uygulama kullanıcı kimlik doğrulaması gerektiriyorsa, kullanıcı kimlik doğrulaması başlamadan önce uygulama ve/veya cihaz bütünlük kontrolleri tamamlanmalıdır.
18. Gizli veya daha yüksek Citi sınıflandırmasına sahip, Citi mülkiyetindeki bilgilere erişen/bunları işleyen/saklayan ve/veya IS risk sınıflandırması Orta veya daha yüksek olan mobil uygulamalar {yalnızca güçlü biyometrik yöntemlerden yararlanmalıdır (ör., ilgili [Android Compatibility Definition Document](#)'ta tanımlanan Class 3 / Strong kategorisini karşılamalı veya aşmalıdır).

19. Mobil uygulamalar, Ortadaki Adam (MitM) saldırılarına karşı koruma sağlamak için karşı önlemler uygulamalıdır.
20. Mobil uygulamalar, bunlarla sınırlı olmamak üzere, 'jailbreak'li veya 'root'lanmış mobil cihazları içeren, güvenliği ihlal edilmiş cihazları tespit edebilmeli ve işletmenin risk değerlendirmesi ve düzenleyici gereksinimlerine uygun şekilde tepki verebilmelidir.
21. Mobil uygulamalar, yazılım belirticinin (ör., mülkiyet kanıtı) klonlanmasını önlemek için güçlü cihaz bağlama uygulamalıdır.
22. Mobil uygulamalar, güvenli klavye uygulamalarını/çözümlerini (ör., mobil işletim sistemleri tarafından yerleşik/önceden yüklenmiş olanlar) kullanmalıdır.
23. Anında bildirimler hiçbir hassas bilgi içermemelidir (ör., Gizli veya daha yüksek olarak sınıflandırılan Citi bilgileri). Ancak tek kullanımlık şifre (OTP), anlık bildirim yoluyla dağıtılabilir.
24. Mobil uygulama çözümleri, bilinen/istismar edilebilir güvenlik açıklarına sahip uygulama sürümlerini kullanan mobil istemcilerle iletişim girişimlerini reddetme/yok sayma yeteneğine sahip olmalıdır.
25. Mobil uygulamalar, [OWASP Mobile Top 10](#) kapsamında yayımlanan önleme teknikleri dâhil ancak bunlarla sınırlı olmamak üzere endüstrinin en iyi uygulamalarına uymalıdır.
26. Yapay zekâ ve makine öğrenimi (AI/ML) tekniklerinden yararlanan mobil uygulamalar, bunu etik biçimde ve Madde 19 - **Error! Reference source not found.** (Üretken Yapay Zekâ/Ajan Yapay Zekâ dâhil) hükümlerine uygun olarak yapmalıdır.
27. Mobil uygulama, Citi'nin yararlandığı amaç/amaçları/işlevleri gerçekleştirmek için gerekli olan asgari cihaz izinlerinden yararlanmalıdır.
28. Mobil uygulamalar, kamuya açık olmayan bilgileri SD kartlar gibi harici/çıkarılabilir depolama birimlerinde saklamayacaktır.**Error! Reference source not found.**

17.65 Yazılım Açıklaması

Tedarikçi, Citi'ye sağlanan tüm ürün veya hizmetlerde yer alan açık kaynak yazılımlar da dâhil olmak ancak bunlarla sınırlı olmamak üzere, her türlü yazılım bileşenini (hepsi birlikte "Yazılım Bileşenleri") ifşa edecektir. Tedarikçi, her durumda Citi'ye önceden açıklama yapmaksızın, güncelleme, yükseltme veya başka bir yolla Citi Sistemlerine kurulacak ürün ya da hizmetlerin herhangi bir sürümüne Yazılım Bileşenleri eklemeyecektir. Ayrıca Tedarikçi, ürünlerinin veya hizmetlerinin, Citi'yi veya Bağlı Kuruluşlarını, Citi tarafından bir Sözleşmede açıkça açıklanmayan ve kabul edilmeyen herhangi bir yükümlülüğe tabi kılan herhangi bir koşul kapsamında lisanslanan Yazılım Bileşenlerini içermemesini sağlayacaktır. Tedarikçi, keşfedilmesinin ardından 30 gün içinde Tedarikçinin kuruluşu, ürünleri veya hizmetleri içinde tespit edilen kötü amaçlı Yazılım Bileşenlerini Citi'ye açıklayacaktır. Tedarikçi özellikle, Citi'ye OWASP CycloneDX dosya biçiminde veya ISO/IEC 5962:2021 Software Package Data Exchange ("SPDX") specification dosya biçiminde bir Yazılım Malzeme Listesi ("SBOM") sağlayarak, ürünlerin veya hizmetlerin her bir sürümünde Yazılım Bileşenlerini kullandığını

açıklayacaktır. Bu gibi bir açıklama, Yazılım Bileşeninin nereden kaynaklandığı (ör. ticari satıcı, gömülü veri tabanı, genel ikili paket yöneticisi, kaynak kodundan derlenmiş bileşenler veya herhangi bir Gömülü Yazılım ya da kürate edilmiş Yazılım Bileşenleri sağlayıcısı) ve Tedarikçinin veya yazılım tedarik zinciri bağımlılıklarından herhangi birinin Yazılım Bileşenlerinin (“çatal” olarak bilinir) bir kopyasını alıp almadığı ve daha sonra bunu bir paket bağımlılığı olarak ya da ürünler ve hizmetlerin derlendiği Tedarikçinin kaynak koduna entegre edilmiş kaynak kodu olarak ürün veya hizmetlerine yerleştirip yerleştirmedeğini belirtmelidir.

17.66 Tehdit Modelleme

Tedarikçi, aşağıdakilerin tümünü kapsamlı bir şekilde ele alan ve/veya içeren bir tehdit modelleme süreci uygulamalıdır:

1. Kapsam Tanımı: Tedarikçi, Citi Gizli ve daha yüksek gizlilik derecesine sahip bilgileri işleyen, saklayan veya ileten yazılım bileşenlerine ve veri akışlarına odaklanarak tehdit modelinin kapsamını açıkça tanımlamalıdır.
2. Tehdit Tanımlama: Tedarikçi, tasarım yaşam döngüsünün başlarında çeşitli saldırı vektörleri ve tehdit aktörlerini dikkate alarak, yazılımın tasarımı, mimarisi ve amaçlanan kullanımı ile ilgili potansiyel tehditleri ve güvenlik açıklarını sistematik olarak belirlemelidir.
3. Risk Analizi: Tedarikçi, potansiyel etkilerini ve olasılığını değerlendirmek için belirlenen tehditleri analiz etmeli ve güvenlik risklerinin önceliklendirilmesini sağlamalıdır.
4. Kontrol Entegrasyonu: Tedarikçi, önceliklendirilen bu riskleri ele almak için uygun güvenlik kontrollerini ve risk azaltma stratejilerini tanımlamalı ve yazılımın tasarımına ve geliştirilmesine entegre etmelidir.
5. Dokümantasyon: Tedarikçi, tespit edilen tehditler, ilişkili riskler ve uygulanan ilgili azaltma önlemleri dâhil olmak üzere tehdit modelini belgelemelidir.
6. Periyodik İnceleme: Tedarikçi, özellikle yazılımın tasarımı, işlevselliği veya dağıtım ortamında önemli değişiklikler olduğunda tehdit modellerini düzenli olarak gözden geçirmeli ve güncellemelidir.

17.67Yapay Zekâ

1. Tedarikçiler, Citi'ye sağlanan veya Citi ile entegre edilen tüm AI/ML sistemleri ve bileşenleri için sağlam bir Güvenli Yazılım Geliştirme Yaşam Döngüsü (SSDLC) uygulamalı ve bunlara uymalıdır. Bu durum, güvenli tasarım, geliştirme, test, dağıtım ve devam eden bakımı içerir.
2. Tedarikçi tarafından sağlanan AI sistemleri, işleyişlerinde bütünlük göstermeli ve hasmane saldırılara karşı güçlü direnç sergilemelidir. Buna, istem enjeksiyonunun tespit edilmesine, girdilerin temizlenmesine ve veri yalıtımının sürdürülmesine yönelik mekanizmaların uygulanması dâhildir.
3. Tedarikçiler tarafından sağlanan AI ajanları ve bileşenleri, Citi sistemleri ve diğer araçlarla güvenli biçimde etkileşim kurmalıdır. Bu durum güçlü kimlik ve erişim yönetimini, araç yürütme argümanlarının katı şekilde doğrulanmasını ve yüksek riskli araç operasyonlarının izole edilmesini gerektirir. Hassas veya yüksek riskli eylemler için Sürece İnsan Müdahalesi (HITL) mekanizmaları dâhil edilmelidir.

4. Tedarikçinin AI sistemleri, tüm önemli olaylar için kapsamlı, değiştirilemez ve denetlenebilir günlükler oluşturmalıdır. Bu günlükler kurcalamadan korunmalı, toplanmalı ve Citi'nin politikalarına uygun olarak saklanmalıdır. Güvenlikle ilgili olayları ve şüpheli aktiviteleri belirlemek ve uyarı vermek için sürekli izleme ve anormallik tespit yetenekleri gerekir.
5. Tedarikçi AI sistemleri, uygun müdahaleye izin vererek risk bazlı insan denetimini desteklemeli ve AI çıktıları ve eylemleri için net hesap verebilirlik ile tasarlanmalıdır. Bu, AI çıktılarını risk seviyesine göre sınıflandırmayı ve insanın müdahale edip geçersiz kılma yeteneklerini desteklemeyi içerir.
6. Tedarikçiler tarafından sağlanan tüm AI ajanları, bileşenleri ve sistemleri güçlü kimlik ve erişim yönetimi kontrolleri uygulamalıdır. Her AI etkileşiminin, tüm erişim için gerekli olan kimlik doğrulaması ile tanımlanabilir bir kimliğe (insan veya insan olmayan) atfedilebilir olması gerekir. AI ajanları, Citi kaynaklarına erişirken yönetilen kimlikler kullanılmalı ve en az ayrıcalık ilkelerine uymalıdır.
 - a. Tedarikçiler, Citi güvenlik politikalarının uygulanmasını, merkezî kimlik yönetimini ve denetlenebilirliği sağlamak amacıyla tüm AI ajanlarına Citi Object Identity Network (COIN) ajan kimlikleri atanmasını, bu kimliklerin Citi Identity and Access Management (IAM) sistemleriyle federasyonunun kurulmasını sağlamalı ve gerekli tanımlamaları yapmalıdır.
 - b. Tedarikçiler, güvenli ağ geçitleri (SSG Gateway veya Apigee gibi) üzerinden sunulan COIN API dâhil olmak üzere Citi onaylı entegrasyon mekanizmalarını kullanarak üçüncü taraf ajanları COIN'e dâhil etmeli ve bu sürecin Citi'nin geçerli güvenlik gerekliliklerine uygun biçimde güvenli olarak yürütülmesini sağlamalıdır.
 - c. Tedarikçiler, kurum içinde barındırılmaları durumunda COIN ile uyumlu kendi belirteçlerini oluşturmalıdır; kurum dışında barındırılan ve kendi birleşik belirteçleriyle gelen isteklerde kimlik doğrulayan Tedarikçilerin ise Citi belirteçleri için desteklenen bir belirteç değişimine sahip olmaları gerekir (örneğin MSFT belirteçlerinden COIN belirteçlerine değişim yapılması). Şu anda değişim mekanizması aracılığıyla desteklenmeyen her türlü yeni belirteç türü, onay için Citi IAM ekibi tarafından gözden geçirilmelidir.
7. Tedarikçilerin Model Context Protocol (MCP) sunucuları veya istemcileri kullandığı ya da sağladığı durumlarda, tüm isteğe bağlı özellikler dâhil olmak üzere MCP RFC 7591'i uygulamaları zorunludur.
8. Tedarikçi AI sistemleri, sistem yönergelerini ve dâhilî çalışma mekanizmalarını ifşaya veya manipülasyona karşı korumalıdır. Bağlam yönetimi, kiracılar, kullanıcılar veya ortamlar arasında veri sızıntısını önlemek için kesin sınırları uygulamalıdır.
9. Tedarikçiler; hasmane saldırılar, model manipülasyonu, yetkisiz AI eylemleri veya AI sistemleriyle ilgili veri ihlalleri dâhil olmak üzere AI'a özgü güvenlik olaylarını tespit etmek, bunlara müdahale etmek ve bunları bildirmek için belgelenmiş prosedürlere sahip olmalıdır. Bu tür olaylar derhâl Citi'ye bildirilmelidir.

18 GÜVENLİ İŞ YERİ KURALLARI

Citi Bilgilerine erişen/bunları işleyen/depolayan/yöneten VE/VEYA Citi markalı internete dönük uygulamaları barındıran VE/VEYA Citi'nin ağ kaynaklarına bağlantısı olan VE/VEYA Citi tesislerine refakatçisiz erişime ihtiyacı olan Tedarikçiler için geçerlidir.

Tedarikçiler, Citi ve Müşterilerinin maddi ve maddi olmayan varlıklarını korumak zorundadır. Citi ve Müşteri varlıkları yalnızca onaylı amaçlar için ve onaylı şekillerde (örneğin, geçerli lisanslara, şartlara ve koşullara uygun olarak) ve yalnızca Citi ve Citi Tedarikçilerinin ticari amaçları doğrultusunda kullanılabilir. Varlıklar arasında nakit, menkul kıymetler, fiziksel mülk, hizmetler, iş planları, Citi Bilgileri, Tedarikçi bilgileri, dağıtımıcı bilgileri, fikrî mülkiyet (bilgisayar programları, modeller ve diğer öğeler) ve diğer tüm kişisel, tescilli ve Gizli Bilgiler yer alır. Citi varlıklarının kötüye kullanılması veya yetkisiz bir şekilde ifşa edilmesi, Citi'ye karşı olan görevinizin ihlali anlamına gelir ve Citi'ye karşı bir dolandırıcılık eylemi teşkil edebilir. Benzer şekilde, Citi varlıkları bağlamında dikkatsizlik, israf veya yetkisiz kullanım da Citi'ye yönelik görevinizin bir ihlalidir.

Öge	Gereklilikler
Citi Bilgileri (elektronik ve basılı dokümantasyon)	Normal çalışma saatleri dışında ve Tedarikçi belirlenen çalışma alanından uzakta olduğunda Citi Bilgilerini kilitleyin ve güvenli bir yerde saklayın.
Masaüstü Kişisel Bilgisayarlar (PC'ler) ve Dizüstü Bilgisayarlar	Herhangi bir Citi Bilgisine erişmek veya görüntülemek için kullanılan PC'ler ve dizüstü bilgisayarlar, belirli bir süre işlem yapılmadığında ekran koruyucu şifreleriyle güvence altına alınmalıdır. Tedarikçi belirlenen çalışma alanından uzaklaştığında PC ve/veya dizüstü bilgisayarını CTRL + ALT + DEL tuşlarına basarak kilitlemeli ve "Bilgisayarı Kilitle"yi seçmelidir. Bir Tedarikçi Citi Bilgilerini görüntülemek için bir dizüstü bilgisayar kullanıyorsa, Tedarikçi söz konusu dizüstü bilgisayarın çalışma saatleri sırasında kablo veya güvenlik kilitleri aracılığıyla ana üniteye sabitlendiğinden ve normal çalışma saatleri sonrasında güvenli bir şekilde kilitlendiğinden emin olmalıdır.
Kilitle	Citi Bilgilerinin saklandığı dosya dolapları ve çekmeceler normal çalışma saatleri dışında kilitlenmelidir.
Açık Ofis Alanları	Açık ofis alanları, Citi Bilgilerini depolamak için dosya sunucusu/mini veri merkezi olarak kullanılmamalıdır; ancak bu amaçla özel olarak tasarlanmış ve Citi tarafından belgelendirilmiş olmalıdır.
Yazıcılar, Fotokopi Makineleri ve Faks tepsileri	Citi ile ilgili tüm materyaller yazıcılardan, fotokopi makinelerinden ve faks tepsilerinden temizlenmelidir.
İmha etmek	Artık gerekli olmayan Citi Bilgilerini imha edin (belirli kayıt tutma çizelgelerini izleyin). Belgeler öğütülmeli veya güvenli/kilitli geri dönüşüm kutularına konulmalıdır. Manyetik medyalar, uygun silme prosedürleri uygulandıktan sonra güvenli biçimde imha edilmelidir.

19 YAPAY ZEKÂ/MAKİNE ÖĞRENİMİ (ÜRETKEN YAPAY ZEKÂ/AJAN YAPAY ZEKÂ DÂHİL)

Tedarikçilere yönelik bu Gerekliliklerde Citi tarafından tanımlandığı şekliyle, sağladıkları ürünün/hizmetin herhangi bir bölümünde Üretken Yapay Zekâ/Ajan Yapay Zekâ dâhil Yapay Zekâ/Makine Öğrenimi (AI/ML) kullanan Tedarikçiler için geçerlidir.

19.1 Tedarikçi, Taraflar arasında Sözleşme kapsamındaki ilgili Ek veya İş Emrinde aksi kararlaştırılmadıkça, aşağıda açıklanan Yapay Zekâ/Makine Öğrenimi (AI/ML) teknolojilerini kullanmayacak ve hiçbir Alt Yüklenicinin de kullanmamasını sağlayacaktır:

- a. Citi'ye doğrudan veya dolaylı olarak sağlamak üzere Sözleşme kapsamında oldukları herhangi bir ürün veya hizmette veya burada yer alan veya gömülü olan herhangi bir üçüncü taraf ürün veya hizmeti dâhil olmak üzere herhangi bir bölümünde kullanılan, kapsanan veya başka bir şekilde dâhil edilen; veya
2. Bu tür AI/ML'nin Citi'ye teslim edilen gerçek ürün veya hizmette kullanılmış, kapsanmış veya başka bir şekilde dâhil edilmiş olup olmadığına bakılmaksızın, Tedarikçinin herhangi bir Sözleşmeyi ifasında herhangi bir şekilde kullanılan; veya
3. Tedarikçinin ticari olmayan iş operasyonlarında (ör., iş kayıtlarının tutulması, süreç iyileştirmeleri, araştırma ve geliştirme, uyum ve iç denetim) kullandığı AI/ML dâhil ancak bununla sınırlı olmamak üzere, Citi Bilgilerini söz konusu AI/ML'ye maruz bırakabilecek herhangi bir biçimde Tedarikçi tarafından kullanılan.

19.2 Tedarikçinin bu yükümlülüklerle uymaması, bu Sözleşmenin şartlarının esaslı ihlali olarak kabul edilecektir.

19.3 Ürünün/hizmetin herhangi bir bölümünde AI/ML kullanımına ilişkin düzenleyici inceleme veya adli soruşturma kapsamında bir regülatörün talepte bulunması hâlinde Tedarikçi; AI/ML modellerini oluşturan algoritmaların fiilî işleyişini ortaya çıkarmak için gerekli algoritma denetimlerinin yürütülmesi ve/veya kolaylaştırılması dâhil olmak üzere regülatörün talebine yanıt verme konusunda Citi'ye yardımcı olmalıdır.

19.4 Aşağıdaki ilkelere de uyulmalıdır:

Yasalılık. Tedarikçi AI/ML, Geçerli Yasalara uyacaktır.

Amaç ve Orantılılık. Tedarikçi, İçeriği veya Citi Bilgilerini Tedarikçi veya herhangi bir üçüncü taraf verisiyle birleştirmeyecektir. Tedarikçi, Citi'nin yazılı onayı olmadan İçeriği veya Citi Bilgilerini AI/ML'yi eğitmek için kullanmayacaktır. Tedarikçi AI/ML, Hizmetlerin sağlanması için gerekli olan durumlar haricinde İçeriği veya Citi Bilgilerini kullanmayacaktır.

20 MÜŞTERİ ŞİKÂyetLERİ

20.1 Şikâyet, bir Müşteri, Müşteri olmayan, potansiyel Müşteri, Citi müşterisi, potansiyel Müşteri veya Müşterinin yetkili temsilcisi (toplu olarak "Müşteri") tarafından Citi Politikası, Citi tarafından veya aracılığıyla sunulan ürün veya hizmet, bir Citi çalışanı, Citi yüklenicisi veya Citi adına hareket eden üçüncü taraf hizmet sağlayıcısı veya yukarıdakilerin herhangi bir kombinasyonu hakkında sözlü veya yazılı olarak (yüz yüze veya telefonla) veya yazılı olarak (posta yoluyla veya e-posta, sohbet veya sosyal medya gibi elektronik iletişimler yoluyla) alınabilen, memnuniyetsizliğini ifade eden sözlü veya yazılı bir iletişimdir.

20.2 Tedarikçiler, Citi Müşteri Şikâyet İşleme Politikası'na ve geçerli Citi Şikâyetle ilgili Standartlar ve Prosedürlere uymalıdır. Tedarikçi, Citi adına sunduğu Hizmetlerle veya başka bir şekilde Citi ile ilgili olarak herhangi bir Müşteriden (veya Citi Şikâyet tanımı uyarınca Müşteri Olmayan ya da potansiyel Müşteriden) veya herhangi bir Regülatörden aldığı yazılı ya da sözlü memnuniyetsizlik veya endişe bildirimini (her biri bir "Şikâyet"), yirmi dört (24) saat içinde birincil Citi iş irtibat kişisine (veya vekiline) yazılı olarak bildirecektir. Citi, Tedarikçiye böyle bir sistem sağlamadığı sürece, Tedarikçi ayrıca Şikâyetleri izlemek ve Citi'ye kendi takdirine bağlı olarak raporların bir kopyasını veya sisteme erişimi sağlamak için Citi'yi makul ölçüde tatmin edecek bir sistem ("İzleme Sistemi") geliştirecek, uygulayacak ve sürdürecektir. İzleme Sistemi:

- Şikâyetleri türlerine, alındıkları tarihe ve Şikâyet bildiriminin Citi'ye iletildiği tarihe göre kategorize edecek,
- Şikâyetin sonuçlanmasına/çözümlemesine kadar olan süreci takip edecek ve
- Citi tarafından makul bir şekilde talep edilebilecek diğer tüm hususları karşılayacaktır. İzleme Sistemi, Tedarikçinin belirli bir konu ile ilgili olarak aşırı sayıda Şikâyet alıp almadığını belirlemesine olanak sağlayacak şekilde tasarlanmalıdır; böylece Tedarikçi (Citi ile istişare hâlinde) Tedarikçinin işletmesi veya Hizmet sunumu ile ilgili sistemik bir sorun olup olmadığını belirleyebilir ve sorunları derhâl düzeltebilir.

21 KİŞİSEL TİCARET VE YATIRIM POLİTİKASI

Citi'nin Kişisel Ticaret ve Yatırım Politikası (PTIP), izin verilen ve yasaklanan ticaret ve yatırım faaliyetlerini, ön izin gerekliliklerini ve Kapsanan Kişinin aracılık veya ticaret

hesaplarının bakımı, ifşası ve gözetimine ilişkin gereklilikleri tanımlar. Bir bireyin Citi ile olan pozisyonunun veya ilişkisinin uygunsuz kullanımını önlemek için kanun ve regülasyonlarla uyumu teşvik etmek amacıyla asgari standartları belirler; buna bireyin (1) Citi veya üçüncü bir taraf ile ilgili Önemli Kamuya Açık Olmayan Bilgi veya içeriden bilgi (toplu olarak “MNPI” olarak anılır) veya (2) müşterilerin menkul kıymetleri, türevler ve emtia pozisyonları, işlemleri ve stratejileri ile ilgili bilgiler dâhildir.

Citi'deki iş sorumluluklarının bir parçası olarak MNPI'ye düzenli erişim gerektiren ve Kapsanan Kişiler ve/veya Citi Erişim kişileri olarak belirlenen tüm Tedarikçi personeli, PTIP kapsamındaki gerekliliklere uymalıdır. Tedarikçi personeli, ICRM'nin kişisel hesap ifşası, kişisel ticaret faaliyetlerinin ön onayı ve kişisel ticaret kısıtlamaları ve periyodik beyanların sunulması ile ilgili taleplerine uymak zorundadır.

22 FATURALANDIRMA VE FATURALAMA STANDARTLARI

Citi'nin hizmet zamanlamasını iyileştirme ve kontrolleri geliştirme çabalarıyla bağlantılı olarak, tüm Tedarikçiler aşağıda ayrıntılı olarak açıklandığı gibi Citi'nin tercih edilen fatura gönderme yöntemlerini ve tercih edilen fatura ödeme seçeneklerini destekleyecektir:

- Tedarikçi, Citi'nin Tedarikçiye ilettiği formatta Citi'ye iletilecek elektronik dosyalar oluşturacak ve/veya Citi iSupplier aracını kullanarak Citi'ye daha sonra dijital olarak iletilmek üzere gerekli fatura/faturalandırma verilerini girecektir.
- Tedarikçi, Tedarikçiye elektronik ödemeyi kolaylaştırmak ve/veya Citi'nin Sanal Kart ödemeleri teklifini (mevcut olduğu durumlarda) kullanmak için Citi'ye gerekli tüm bankacılık bilgilerini ve destekleyici belgeleri sağlayacaktır.

Not: Ödeme koşulları, fatura gönderiminin Citi'ye ulaştığı tarihten itibaren hesaplanır.

Citi, zamanında ödeme yapmak ve sözleşmesel taahhütleri yerine getirmek için tüm Tedarikçilerin, Citi'ye mal veya hizmetler için fatura gönderirken aşağıdaki fatura verilerini eklemelerini ve ilgili yönergelere uymalarını şart koşturmaktadır:

1. Doğru Citi ticari kuruluşu, “Fatura adresi” ve ilişkili Citi ticari iletişim kişinin adı.
2. Fatura Numarası, Fatura Tarihi ve Satın Alma Sipariş Numarası.
3. Faturalar Citi satın alma siparişinde belirtilen Citi lokasyonuna veya e-posta adresine gönderilmelidir.
4. Faturalandırılan mal veya hizmetin faturada açık ve tanımlayıcı bir şekilde belirtilmesi gerekmektedir.
5. Yalnızca belirli fatura için geçerli ücretleri ekleyin (diğer bekleyen ödenmemiş fatura bakiyelerini eklemeyin).
6. Faturalar destekleyici belgeler dâhil olmak üzere İngilizce dilinde düzenlenmelidir.

23 ZORUNLU UZAKLAŞTIRMA POLİTİKASI

Citi'nin Zorunlu Uzaklaştırma Politikası düzenlemesi, özellikle şirketin ticari defterlerini ve kayıtlarını etkileyen hassas veya yüksek riskli aktiviteleri yürüten kişilerin, belirli aralıklarla bu görevlerinden uzaklaşmasını gerektirir. Uygulanan bu zorunlu ayrılık, aksi takdirde gizli kalabilecek olası dolandırıcılık, hırsızlık veya diğer usulsüzlükleri tespit etme fırsatları yaratarak dâhilî kontrolleri güçlendirmeyi amaçlar. Bu politika, ABD Federal Rezerv Kurulu tarafından hassas pozisyonlardaki personel için zorunlu uzaklaştırmalara ilişkin belirlenen denetim beklentileriyle uyumludur.

Citi'deki iş sorumlulukları kapsamında hassas verilere erişen ve “Hassas” kişiler olarak tanımlanan tüm Tedarikçi personeli, MA policy kapsamındaki gerekliliklere uymalıdır. Hassas personelin her yıl tüm politika kural ve kısıtlamalarına uyarak bir Zorunlu Uzaklaştırma Dönemi planlaması ve bu dönemi eksiksiz tamamlaması gerekir. Bu süre zarfında söz konusu personel, hassas nitelikteki hiçbir faaliyeti yürütemez, talimat veremez, yetkilendiremez veya onaylayamaz, talepleri kapsama dâhilindeki kişilere yönlendirmek dışında müşteri etkileşimleri dâhil hiçbir iletişime esasa ilişkin yanıt veremez. Uzaklaştırma döneminin başladıktan sonra kesintiye uğraması gerekirse, sistem erişiminin yeniden sağlanabilmesi için yöneticiler veya Citi iş irtibat kişileri bu dönemi Uyum sistemlerinde iptal etmelidir; ardından Çalışan yeni bir uzaklaştırma dönemi planlamalıdır.

EK - TANIMLAR

Hava Boşluğu, bir bilgisayar, sistem veya ağın diğer bilgisayar, sistem veya ağlardan fiziksel olarak ayrıldığı bir güvenlik önlemidir. Hava boşluklu bir veri yedekleme mimarisi, siber saldırıya maruz kalmayı sınırlandırır ve verilerin saldırı başlamadan önceki bir zamana geri yüklenmesine olanak verir.

Geçerli Kanun şunları içerir: (a) eyalet düzeyindeki haciz yasaları ve regülasyonları ile (b) Fair and Accurate Credit Transactions Act of 2003'ün 114. maddesini uygulayan Office of the Comptroller of the Currency dâhil olmak üzere çeşitli United States Federal Agencies tarafından yayımlanan kurallar, kılavuzlar ve diğer duyurular (bazen Red Flag Guidelines and Regulations olarak anılır)

Erişilebilirlik Alanı, Bulut Hizmeti Sağlayıcının bir grup mantıksal veri merkezine sahip olduğu yerdir. Erişilebilirlik Alanı, bir Bulut Bölgesinde yedekli güç, ağ iletişimi ve telekomünikasyona sahip bir veya daha fazla ayrı veri merkezidir.

Yapay Zekâ (AI), klasik istatistiksel, matematiksel, ekonometrik veya finansal yaklaşımların ötesine geçen şekillerde tahminler, öngörüler, öneriler veya kararlar almak için bilgisayar programları aracılığıyla insan zekâsını taklit eden nicel bir yöntem, sistem veya yaklaşımı ('teknikler') ifade eder. Bu, aşağıda belirtilen tüm AI kategorilerinin yanı sıra AI değişikliklerini de içerir - örneğin: Üretken Yapay Zekâ, Ajan Yapay Zekâ, Büyük Dil Modelleri, Genel Amaçlı Yapay Zekâ (GPAI) Modelleri vb.

AI Kategorileri şunları içerir:

- **Statik AI:** Çevrim dışı olarak manuel şekilde eğitilen veya parametreleri açıkça programlanan ve ardından değerlendirmeler, tahminler, öneriler veya kararlar vermek için kullanılan yapay zekâ teknikleri.
- **Dinamik AI:** "Statik AI"dan farklı olarak, üretimde parametreleri periyodik olarak otomatik şekilde yeniden eğitebilen teknikler.
- **Otomatik AI:** Temel yapılarını (örneğin hiperparametreler, giriş değişkenleri) otomatik olarak değiştirebilen "Dinamik AI" teknikleri.
- **Bilişsel Yapay Zekâ:** Özel olarak eğitilmedikleri konularda bile özerk olarak karar verebilen ve buna göre hareket edebilen teknikler.

Makine Öğrenimi (ML), her parametre gösterimini veya bilgisayar adımını açıkça programlamadan verilerden gösterimler ya da çıkarımlar türeten AI alt kümesidir; örneğin Random Forests ve Neural Network tabanlı yaklaşımlar. Buna karşılık, ML alt kümesinin üyesi olmayan AI teknikleri arasında bulanık mantık, doğal dil işleme için karmaşık bağımlılık ayrıştırma teknikleri gibi teknikler yer alır.

Ticari Aktivite Sahibi (BAO), Tedarikçi ilişkileri ile bağlantılı belli aktiviteleri gerçekleştirmek ve aktif olarak yönetmekten sorumlu bir Citi çalışanıdır.

İş Tanıtıcısı Citi adına yeni iş fırsatları belirlemek veya mevcut müşteri ilişkilerini yönetmek üzere Citi tarafından görevlendirilen bir Tedarikçidir.

İş Hediyesi, genellikle 25 ABD\$ veya daha az değerdeki öğeleri hariç tutan Citi'nin işi veya dış tarafın işi ile bağlantılı olarak bir Citi çalışanı tarafından verilen veya alınan değerli herhangi bir öğedir (İş Amaçlı Ağırılama dışında).

Citi Bilgileri, Citi'nin sahip olduğu veya hem dijital hem de dijital olmayan formatlarda depolama, işleme, iletim veya elden çıkarma sırasında korumakla yükümlü olduğu bilgilerdir.

Tedarikçiler için Citi Gereklilikleri

Citi Bilgileri Sınıflandırmaları şunları içerir:

Gizli, Citi işletmeleri ve/veya ilgili taraflar hakkında bireylere atıfta bulunmayan ve yüksek düzeyde koruma gerektiren Bilgilerdir. Bu bilgilerin gizliliğinin, bütünlüğünün veya kullanılabilirliğinin ihlal edilmesi; Citi'nin operasyonları, mali durumu, franchise'ı veya kurumsal müşterileri üzerinde ciddi etki yaratabilir.

Gizli Kişisel Tanımlayıcı Bilgiler, Kimlik hırsızlığı, kredi dolandırıcılığı veya söz konusu kişiye karşı diğer mali dolandırıcılık gibi yasa dışı aktiviteleri kolaylaştırma potansiyeli olan bir birey hakkındaki kişisel bilgilerdir. Bu bilgilerin gizliliğinin, bütünlüğünün veya kullanılabilirliğinin ihlal edilmesi; mali kayıp veya dolandırıcılık dâhil ancak bunlarla sınırlı olmamak üzere ilgili kişi veya kişiler üzerinde önemli etki yaratabilir.

- Diğer kişisel verilerle birleştirildiğinde Gizli PII oluşturan kişisel veri ögeleri, aşağıdakilerle birlikte bireysel adı veya iletişim bilgilerini (adres, telefon veya e-posta adresi) içerir:
 - Fon hareketleriyle sonuçlanabilecek veya kimlik hırsızlığı veya sahtekârlık yapmak için kullanılacak işlem verileri ögeleri, örneğin:
 - Kredi/Banka kartı numarası.
 - Kart Doğrulama Değeri (CVV) veya PIN
 - Kredi raporu verileri (kredi puanı)
 - Tam doğum tarihi
 - Çalışan performansı (değerlendirme/geri bildirim) veya ücret bilgileri
 - CCTV ve ATM kayıtları dâhil olmak üzere video kayıtları
- Belirli kişisel veri unsurları tek başına Gizli PII oluşturmaktadır:
 - Bir ABD Sosyal Güvenlik numarası, devlet tarafından verilen kimlik numarası (kullanım ve/veya yasal koruma statüsü bakımından ABD Sosyal Güvenlik numarası eş değeri), pasaport numarası, sürücü belgesi numarası veya bir kişinin vergi kimlik numarası

Dâhilî, bir kişiye ilişkin olmayan, iş amaçlı olan ve orta düzeyde koruma gerektiren bilgilerdir. Bu bilgilerin gizliliğinin, bütünlüğünün veya kullanılabilirliğinin ihlal edilmesi, bir ekip veya çalışma grubu üzerinde **sınırlı etki** yaratabilir.

- **Kişisel Tanımlayıcı Bilgiler (PII)** Kişisel Bilgiler aşağıdaki özellikleri taşıyan bilgilerdir:
 - Bir kişiyi veya haneyi tanımlar ya da tanımlamak için kullanılabilir (ör., ad, imza, adres, sosyal güvenlik numarası veya ikamet kayıt numarası gibi benzersiz ulusal tanımlayıcı, doğum tarihi, sürücü belgesi numarası).
 - Bir kişi veya haneyle ilgilidir, onu tanımlar, onunla ilişkilendirilebilir veya makul olarak (doğrudan ya da dolaylı biçimde) onunla bağlantılandırılabilir;
 - Bir şahsın kimliğini doğrulamak veya bir hesaba erişim sağlamak için kullanılacak olan (ör.,
 - kullanıcı adı, e-posta adresi, parola, PIN, kimlik numarası, güvenlik sorularının yanıtları); veya bir şahısla ilgili olan ve hassas nitelik taşıyabilecek olan (ör., kişisel tıbbi bilgiler veya sağlık bilgileri, hesap numarası, hesap değeri).
 - Kişisel Bilgiler ayrıca Korunan Sağlık Bilgilerini (U.S. Health Insurance Portability and Accountability Act'ta tanımlandığı şekliyle), Hassas Kişisel Bilgileri ve Kredi Bilgilerini (çeşitli veri koruma/gizlilik ve banka gizliliği yasalarında tanımlandığı şekliyle) içerir.

Kamuya Açık, Citi dışında serbest olarak erişilebilir olan veya Citi hakkındaki haberlerde yer alan Citi basın açıklamaları veya makaleler gibi genel kullanım amaçlı olarak öngörülen bilgilerdir.

Kısıtlı, Citi veya bağlı kuruluşları açısından en hassas olan, belirli kişiler ya da gruplarla sınırlı kullanıma sahip ve en yüksek koruma düzeyini gerektiren Bilgilerdir. Bu bilgilerin gizliliğinin, doğruluğunun veya kullanılabilirliğinin tehlikeye atılması, Citi'nin operasyonları, mali durumu, franchise'ları veya kurumsal müşterileri üzerinde **ciddi (firma çapında, birden fazla bölge, birden fazla sektör) etkiye** sahip olabilir.

- **Hassas PII**, belirli yasalarca ek koruma gerektirdiği belirtilen ve potansiyel olarak bir kişiye karşı yasa dışı ayrımcılık yapmak ya da başka bir şekilde haksızlığa veya zarara neden olmak için kullanılabilecek kişisel bilgilerdir. Bu bilgilerin gizliliğinin, bütünlüğünün veya kullanılabilirliğinin ihlal edilmesi, mali kayıp, dolandırıcılık veya ayrımcı etki dâhil ancak bunlarla sınırlı olmamak üzere kişi üzerinde önemli etki yaratabilir.
- Şunlarla özel olarak bağlantılı veriler: ırk, din, dinî veya felsefi inançlar, etnik köken, siyasi bağlantı veya görüşler, sendika üyeliği, cezai geçmiş bilgileri veya ceza gerektiren suçlar, genetik veriler, biyometrik veriler veya bir bireyin cinsel yönelimi veya aktiviteleriyle ilgili veriler.
- Şahsın tıbbi geçmişine veya zihinsel veya fiziksel durumuna ilişkin bilgileri içeren Kişisel Sağlık bilgileri (PHI).

Müşteri, Citi'nin herhangi bir alıcısı veya müşterisi anlamına gelecektir ve bireylerin (diğer deyişle, gerçek kişiler) yanı sıra işletmeleri, kuruluşları, organizasyonları ve tüzel kişilikleri içerebilir.

Bulut Bölgesi, Bulut Hizmeti Sağlayıcının veri merkezlerini kümelediği fiziksel bir konumdur.

İletişim Ekipmanları, Sistemleri ve Hizmetleri, yazılı, sesli veya görüntülü elektronik iletişimlerin iletiminde kullanılan herhangi bir donanım, yazılım veya uygulamadır. eComm Kanalları aşağıdakileri içerir ancak bunlarla sınırlı değildir: "Bring Your Own Device" (BYOD), BlackBerry, telefon, faks (faks hizmetleri), intranet ve internet erişimi, Wi-Fi Hizmetleri, e-posta hizmetleri, Microsoft Lync, Skype ve Bloomberg mesajları gibi anlık mesajlaşma hizmetleri, yerleşik iletişim özelliklerine sahip web siteleri ve uygulamalar, Zoom veya Microsoft Teams gibi görüntülü toplantı ya da iş birliği platformları, sosyal medya hizmetleri, etkileşimli bilgi paylaşım hizmetleri, üçüncü taraf sohbet odaları, elektronik duyuru panoları ve bloglar dâhil olmak üzere bilgisayarlar, dizüstü bilgisayarlar, tabletler, mobil cihazlar veya cep telefonları.

İçerik; Citi'nin Gizli Bilgileri ile (a) Citi veya Bağlı Kuruluşları tarafından ya da bunlar adına veya bunların müşterileri, alıcıları ya da hizmet sağlayıcıları tarafından ya da bunlar adına Tedarikçiye doğrudan veya dolaylı olarak sunulan ya da kullanıma açılan, (b) Hizmetler aracılığıyla oluşturulan veya üretilen ya da (c) yukarıdakilerin herhangi birinden türetilen her türlü diğer veri, rapor, istatistik veya bilgi anlamına gelir.

Sözleşme; iki veya daha fazla tarafça imzalanan ve bir teklif, kabul, karşılık, tarafların yükümlülükleri ve amacın hukuka uygunluğunu içeren yazılı bir hukuki belgedir. Sözleşme örnekleri; ürün ve hizmetlere ilişkin Ana Sözleşmeleri, iş tanımlarını/iş emirlerini, değişiklikleri ve ekleri, çizelgeleri, siparişleri veya bir Citi tüzel kişiliği ile bir Tedarikçi tarafından imzalanan diğer yazılı belgeleri içerebilir. Bir Gizlilik (İfşa Etmeme) Anlaşması (NDA) da bu Standartların amaçları doğrultusunda bir Sözleşme olarak değerlendirilir.

Erişim Reddi (DOA) Testi, tanımlanan RTO içinde kurtarılabilecek Citi iş süreçlerine yönelik Tedarikçi personelini ve desteğini doğrular.

Hizmet Engelleme (DOS) Testi, Tedarikçinin Citi işlerini destekleyen uygulaması ve temel altyapı bileşenlerinin tanımlanan RTO'da kurtarılabileceğini doğrular.

“Mevduat Materyalleri”; Citi ortamında çalıştırılmak üzere Citi'ye lisanslanan yazılım veya Tedarikçinin Citi'ye sağladığı Barındırılan Hizmetlerde kullandığı materyaller bakımından, geçerli olduğu ölçüde, aşağıdaki (i)-(vi) fıkraların tümü anlamına gelir:

- (i) Citi ile yapılan geçerli sözleşmede belirtilen lisanslı yazılımın veya Barındırılan Hizmetlerin geliştirilmesi, işletilmesi, bakımı ve desteği için kullanılan yazılımın Kaynak Kodunun tam, kopyalanmış bir sürümü (ve bu tür yazılımların veya Barındırılan Hizmetlerin tüm sonraki sürümleri) ve bu tür yazılımlara ilişkin tüm Belgeler (Citi'nin bu Kaynak Kodunun parçalarının bir kopyasına zaten sahip olup olmamasından bağımsız olarak) (**“Kaynak Kodu Deposu”**);
- (ii) Tedarikçinin lisanslı yazılımın veya Barındırılan Hizmetlerin geliştirilmesi, işletilmesi, bakımı ve desteği ile ilgili olarak haklara sahip olduğu herhangi bir üçüncü taraf yazılımının Kaynak Kodu;
- (iii) Yazılımı veya Barındırılan Hizmetleri işletmek, sürdürmek ve desteklemek için, Mevduat Materyallerinde yer alan Kaynak Kodunu çalıştırılabilir forma dönüştürmek için gereken hata ayıklayıcılar, derleyiciler ve montajcılar gibi tüm yazılım araçlarının lisanslı bir kopyası;
- (iv) Yukarıda belirtilmeyen ölçüde, aşağıdakileri sağlayan herhangi bir Belge: (A) Mevduat Materyallerinin genel açıklamaları ve işlemleri; (B) mimarisi ve temel program işlevleri; (C) veri akışı bilgileri; (D) ayrıntılı bellek haritası ve listeleme; (E) giriş/çıkış bağlantı noktası haritaları; ve (F) uygulanabilir programlama dilinde/dillerinde sıradan beceriye sahip bir programcının Mevduat Materyallerinde yer alan Kaynak Kodunu kullanmasına ve değiştirmesine olanak sağlayacak diğer ayrıntılar;
- (v) Citi'nin veya Citi adına yetkili bir üçüncü tarafın yazılımı veya Barındırılan Hizmetleri kullanmasını, çalıştırmasını, değiştirmesini ve geliştirmesini sağlamak için makul ölçüde gerekli olacak yazılım veya Barındırılan Hizmetlerle ilgili tüm diğer teknik bilgiler; ve
- (vi) Yazılım veya Barındırılan Hizmetlerle bağlantılı olarak kullanılan tüm üçüncü taraf yazılım ve teknolojilerinin listesi, yazılımda kullanımına ilişkin makul ayrıntılar ve söz konusu yazılım veya teknolojinin sağlayıcısına ilişkin iletişim bilgileri dâhil. Citi, Mevduat Materyallerinin (ii) fıkrasında belirtilenler dışında üçüncü taraflara ait herhangi bir kaynak kodu içermediğini kabul ve beyan eder; ve
- (vii) Barındırılan Hizmetler açısından:
 - a. bulutta barındırılan üretim ortamının ölçeklendirilmiş bir kopyası veya Citi'nin üretim ortamını çoğaltmak için gereken ortama özgü bulutla ilgili materyaller ve diğer bilgiler (ancak bunlarla sınırlı olmamak üzere): kod olarak altyapı; Terraform betikleri, bulut kaynakları, CloudFormation şablonları, yapılandırma dosyaları, bulut kiracıları, bulut abonelikleri, makine imajları, Docker imajları ve yazılımın altyapı kaynak kodu; ve
 - b. yazılım içinde tutulan Citi verilerinin bir kopyası.

Elektronik İletişim, Personel tarafından elektronik araçlar kullanılarak gönderilen, alınan veya kullanılan, kablolu veya kablosuz sinyallerle taşınan mesajlar veya bilgilerdir. Elektronik İletişimler, kısa mesajlar, e-posta, eşler arası veya anlık mesajlar, blog yazıları, sosyal medya gönderileri, WhatsApp, WeChat, Line, Signal veya Viber gibi mesajlaşma uygulamaları aracılığıyla gönderilen mesajları ve ekleri, ekran görüntülerini, kaydedilmiş ses veya video dosyalarını, canlı ses veya videoyu ve Elektronik İletişim Ekipmanları, Sistemleri ve Hizmetleri aracılığıyla oluşturulan, alınan, indirilen, saklanan, iletilen, silinen veya kullanılan dosyaları içerir ancak bunlarla sınırlı değildir.

Fonksiyonel ID'ler, bir güvenlik sistemine erişmek için bir kişi ya da süreç tarafından kullanılan, ADMIN veya ROOT gibi genel bir ID'dir. Kimlik ve Erişim Yönetimi (IAM) operasyonundaki kilit bir öncelik, Citi'nin Fonksiyonel ID'lerin kullanımını çevreleyen risklere karşı koruma sağlamak için özel, tanımlı kontrollere sahip olduğundan emin olmaktır.

Franchise Kritik İşlemler/Franchise Kritik Uygulamaları (FCA), Citi tarafından Franchise Kritik İş Fonksiyonlarının başarılı şekilde yürütülmesi için Citi tarafından zorunlu olarak tanımlanmış olan işlemler/uygulamalardır.

Dolandırıcılık, başkalarını kandırmak için tasarlanmış olan, kurbanın kayıp yaşamasıyla veya failin bir kazanç elde etmesiyle sonuçlanan kasıtlı bir hareket, yanlış beyan veya ihmaldir.

Barındırılan Hizmetler, Yüklenen Uygulamaları ve Barındırılan Hizmetleri, tüm uygulamaları ve diğer yazılımları, veri tabanlarını, web sitelerini, sunucuları, donanımı, ağları, telekomünikasyon ve diğer ekipmanları ve Barındırılan Hizmetler ortamına kurulmuş veya burada kullanılan diğer teknolojileri sağlamak için Tedarikçi tarafından yönetilen veya kullanılan tüm tesisleri ve ortamı ve her durumda, tüm İçerik ve Citi Sistemleri hariç olmak üzere, tüm Güncellemeleri ve Destek Hizmetlerini içerir.

Kimlik Doğrulama Verileri (IVD), Güvenlik Soruları (SQ) veya Bilgi Tabanlı Kimlik Doğrulama (KBA) soruları olarak tanımlanır. Güvenlik Soruları genellikle uygulama tarafından tanımlanır ve son kullanıcı tarafından yanıtlanır. Örnekler annenin kızlık soyadı, doğum yeri, en sevdiği dondurma vb.'dir. Her iki soru türü de Kimlik Doğrulama Verisi olarak değerlendirilmelidir.

Bilgi Güvenliği veya "IS", bir bilgisayarın ya da bilgisayar sisteminin yetkisiz erişim veya saldırıdan korunduğu durum anlamına gelir ve bu durum sayesinde (a) bilgisayar veya bilgisayar sistemi kullanılabilir ve çalışır durumda kalır; (b) bilgisayarın veya bilgisayar sisteminin bütünlüğü korunur ve (c) bilgisayarda ya da bilgisayar sisteminde saklanan, işlenen veya bunlar aracılığıyla iletilen bilgilerin bütünlüğü ve gizliliği korunur.

IS Tehdidi, bir bilgisayar veya bilgisayar sistemi üzerinde veya aracılığıyla gerçekleştirilen ve o veya başka bir bilgisayar veya bilgisayar sisteminin IS'sini tehlikeye atabilecek veya olumsuz yönde etkileyebilecek (bilinen veya şüphelenilen) eylem veya aktivite anlamına gelir.

IS Güvenlik Açığı, bir bilgisayar veya bilgisayar sistemindeki, bir veya daha fazla IS Tehdidi tarafından istismar edilebilecek herhangi bir güvenlik açığı anlamına gelir.

Müşteri Olmayan/Gelir Getirmeyen; yasal, denetleyici, düzenleyici ve İş Sürekliliği faaliyetleri dâhil olmak üzere gelir getirici faaliyetlerle ilişkili olmayan kritik iş faaliyetleri olarak tanımlanır.

Gizlilik Anlaşması (NDA), Citi ile Tedarikçi arasında, Bilgilerin paylaşımı, kullanımı ve açıklamasının anlaşmanın şartları tarafından yönetildiği bir anlaşmadır.

Açık kaynak yazılım; kaynak kodu veya kaynak kodu özgün tasarımına göre kullanılmak ya da değiştirilmek üzere kamuya açık olan derlenmiş bir bilgisayar programı anlamına gelir.

Personel: doğrudan ifade edilmiş veya bağlamdan türetilmiş olsun, Tedarikçi ve bağlı kuruluşları, yöneticileri, yetkilileri, çalışanları, acenteleri, denetçileri, danışmanları, hizmet sağlayıcıları ve yüklenicileri (Citi personeli hariç) anlamına gelir. Tedarikçi personeli ayrıca herhangi bir Alt Yüklenicinin yöneticilerini, memurlarını, çalışanlarını, temsilcilerini, denetçilerini, danışmanlarını veya diğer temsilcilerini de içerir."

Kayıt Envanteri, Citi'nin kayıtlarına ait kayıt türlerini, konumu, tarihleri, vb. içeren ve bir işletmenin Bilgi Yaşam Döngüsü yoluyla kayıtlarını uygun biçimde yönetmek için ihtiyaç duyduğu ayrıntılı bir listedir.

Bilgi Bekletme, bekletme emrini veren makam tarafından kaldırılıncaya kadar değişikliği veya imhayı askıya alan Kayıtlar ve Bilgi için konulan bir şarttır.

Geri Kazanım Kapasitesi, Tedarikçinin ürün ve hizmetlerine ilişkin teslimat hacmi, miktarı veya hızı olup, ürün ve hizmetlerin normal teslimatının yüzdesi olarak ifade edilir.

Kurtarma Süresi, Tedarikçinin kurtarma modundayken operasyonlarını sürdürebileceği takvim günü cinsinden azami süredir.

Kurtarma Noktası Hedefi, bir iş kesintisi sonrasında verilerin kurtarılması gereken, saat cinsinden belirtilen geçmişteki zaman noktasıdır. Büyük bir olay nedeniyle bir BT hizmetinden veri kaybının yaşanabileceği hedeflenen maksimum süredir. RPO, bir BT Hizmetini etkileyen Büyük Bir Olay olması durumunda verilerin kaybolabileceği maksimum zaman diliminin ölçüsüdür. Örneğin, bir önceki günün işlenmesinin sonunda ne kadar verinin kaybolabileceğinin doğrudan bir ölçüsü değildir.

Kurtarma Zamanı Hedefi, bir hizmet kesintisi ve ürünler ile hizmetlerin eski hâline getirilmesi arasındaki saat biriminden süredir.

“Serbest Bırakma Olayı” aşağıdakilerden herhangi biri veya birkaçı anlamına gelir:

- (i) Tedarikçinin (A) ödeme güçlüğüne düşmesi veya borçlarını genel olarak vadeleri geldikçe ödeyemediğini kabul etmesi; (B) yerel veya yabancı herhangi bir iflas ya da ödeme güçlüğü yasası kapsamında, gönüllü ya da gönülsüz olarak, yedi (7) iş günü içinde tamamen durdurulmayan veya başvurudan sonraki kırk beş (45) gün içinde reddedilmeyen ya da iptal edilmeyen bir takibata tabi olması; (C) alacaklıların yararına genel bir devir yapması; veya (D) yetkili bir mahkeme kararıyla, mal varlığının ya da işinin önemli bir bölümünün yönetimini devralmak veya bu bölümü satmak üzere kayyım, müteveli, saklayıcı ya da benzer bir temsilci atanması.

Kaynak Yönetimi Organizasyonu (RMO); Stratejik Kaynak Bulma, Satın Almadan Ödemeye Operasyonlar, Personel Ofisi ve Tedarikçi Yönetim Çerçevesi dâhil olmak üzere Citi'nin küresel, uçtan uca kaynak yönetiminden sorumludur.

RMO Kaynak Bulma Yöneticisi; RFP'ler ve diğer Tedarikçi seçim faaliyetleri, Sözleşme hüküm ve koşullarının idaresi ve mali değerlendirme akreditasyon gereklilikleri dâhil olmak üzere Sözleşmenin ticari şartları, gereklilikleri ve fiyatlandırmasının müzakeresinden sorumlu, Kaynak Yönetimi Organizasyonu (RMO) bünyesindeki kişidir.

Bir kişi üzerinde **Ağır veya Yıkıcı olumsuz etki**; mali kayıp, iş kaybı veya iş bulamama ya da iş bulmakta güçlük çekme, insan haklarının kaybı, kişisel veya kamusal küçük düşürülme veya hukuka aykırı hapis cezası dâhil olmak üzere kişi açısından önemli olumsuz sonuçlara makul olarak yol açabilecek etki anlamına gelir.

Alt Yüklenici: Alt yüklenici, Citi'nin üçüncü tarafla sözleşme yaptığı hizmet veya aktivitelerin bir kısmını veya tamamını gerçekleştirmek üzere üçüncü bir tarafça kiralanan dördüncü taraftır (kişi veya kuruluş).

Rehberlik:

S1: Üçüncü Tarafın tüm alt yüklenicilerinin rapor edilmesi gerekiyor mu?

C1: Yalnızca gerçekleştirilen hizmetle ilgili alt yüklenicilerin raporlanması gerekir. Bir alt yüklenici tarafından gerçekleştirilen hizmet veya aktivitelere örnekler aşağıdakileri içerir, ancak bunlarla sınırlı değildir:

*Citi'nin Üçüncü Tarafla sözleşme yaptığı hizmeti/aktiviteleri doğrudan veya dolaylı olarak destekleyen teknoloji veya yazılım hizmetlerini gerçekleştiren bir alt yüklenici; veya

*Hizmetleri, Gizli veya daha yüksek sınıflandırılmış Citi Bilgilerine erişimi içeren bir alt yüklenici; veya

*Mevcut/potansiyel Citi Müşterisi ile doğrudan veya dolaylı etkileşimi olan bir alt yüklenici; veya

*Refakatsiz olan ve herhangi bir Citi tesisi içinde veya dışında Citi belgelerinin parçalama veya arşivleme hizmetlerini gerçekleştiren bir alt yüklenici; veya

*Ödemeler, tahsilat, borç verme vb. gibi temel bankacılık fonksiyonlarını veya hizmetlerini destekleyen bir alt yüklenici.

Tedarikçi: Bu “Tedarikçilere Yönelik Citi Gereklilikleri” belgesinin amaçları doğrultusunda, “Tedarikçi” yalnızca bir Citi Kuruluşuna doğrudan ürün veya hizmet sağlamak veya bir Citi Kuruluşunun iş hedeflerine ulaşmasını desteklemek için bir iş anlaşması yapan bir Harici Üçüncü Tarafı ifade eder. Haricî Üçüncü Taraf, Citi dışı bir kuruluş olarak tanımlanır. Tedarikçiler ayrıca bir Citi Kuruluşunun müşterisi veya alıcısı olabilir veya Citi müşterileri ve alıcılarıyla etkileşimleri destekleyebilir; ancak, yalnızca Citi’nin müşterisi veya alıcısı olmalarına dayanan düzenlemeler, bu belgenin kapsamında tedarikçi ilişkileri olarak kabul edilmez.

Geçici Bilgiler: Kayıt, Citi’nin yasal, regülasyonel veya onaylanmış ticari nedenlerden dolayı saklamakla yükümlü olduğu bilgilerin nihai ve en eksiksiz versiyonudur. Diğer tüm bilgiler “Geçici Bilgi” olarak sınıflandırılır.