Aşağıdaki çeviri yalnız bilgilendirme amacıyla sağlanmıştır. Bu çeviri ile son güncellenmiş İngilizce sürüm arasında (çeviri gecikmelerine bağlı olanlar dâhil olmak üzere) uyuşmazlık, tutarsızlık veya çelişki olması durumunda İngilizce sürüm geçerli olacaktır.

AMAZON TEDARİKÇİ GÜVENLİK POLİTİKASI

Son güncelleme: Eylül 11, 2024

1. **KAPSAM.** Tedarikçi bu güvenlik gerekliliklerine uyacaktır ("Güvenlik Politikası"). Bu Güvenlik Politikası, Tedarikçinin diğer sözleşmesel veya yasal yükümlülüklerinin hiçbirini sınırlamaz. Tedarikçi, bu Güvenlik Politikası ile Tedarikçi ile Amazon arasındaki başka sözleşmeler arasında bir çelişki olduğu ölçüde, Amazon Bilgilerini daha iyi koruyan daha kısıtlayıcı gerekliliklere uyacaktır.

2. **GÜNCELLEMELER**.

2.1 Amazon, bu Güvenlik Politikasında zaman zaman bu Güvenlik Politikasının "Son güncelleme" tarihinden 30 gün sonra yürürlüğe girecek olan ticari olarak makul güncellemeler yapabilir. Tedarikçi, güncellemeler yürürlüğe girdikten sonra güncellenmiş Güvenlik Politikasının bağlayıcılığını kabul eder.

2.2 Tedarikçi bu güncellemeler yürürlüğe girmeden önce güncellemeler hakkında ön bildirim almak isterse bu Güvenlik Politikası web sayfasında sağlanan abonelik formunu kullanarak güncelleme bildirimlerini almak üzere abone olabilir. Tedarikçi, güncelleme bildirimi aboneliği için verdiği tüm Tedarikçi iletişim bilgilerinin daima güncel ve doğru olmasını sağlayacaktır. Tedarikçi, e-posta ile gönderilmesi halinde güncelleme bildirimini gerçekten alıp almadığına bakılmaksızın herhangi bir güncelleme bildirimini almış sayılacaktır.

3. **İZİN VERİLEN AMAÇ.**

3.1 **Açık Yetki**. Tedarikçi, yalnızca Sözleşme kapsamında açıkça izin verilen Amazon Bilgilerini münhasıran Sözleşme kapsamındaki ürün veya hizmetleri sağlamak amacıyla İşleyebilir ("İzin Verilen Amaç").

3.2 **Veri Saklama**. Tedarikçi, Amazon Bilgilerini yalnızca İzin Verilen Amaç amacı ile ve bunun için gerekli olduğu sürece saklayacaktır.

3.3 **Açık Sınırlamalar**. Tedarikçi: (a) Anonimleştirilmiş olsa bile herhangi bir Amazon Bilgisini İşlemeyecektir; (b) Anonimleştirilmiş olsa bile herhangi bir Amazon Bilgisini herhangi bir üçüncü tarafa devretmeyecek, kiralamayacak, takas etmeyecek, ticaretini yapmayacak, satmayacak, ödünç vermeyecek, kiraya vermeyecek veya başka bir şekilde dağıtmayacak veya kullanıma sunmayacaktır veya (c) Anonimleştirilmiş olsa bile Amazon Bilgilerini kullanarak herhangi bir Yapay Zeka (AI) veya Makine Öğrenimi (ML) modelini geliştirmeyecek, eğitmeyecek veya iyileştirmeyecektir.

4. **ASGARİ GÜVENLİK GEREKLİLİKLERİ**. Tedarikçi, sektörün en iyi uygulamalarıyla (Uluslararası Standardizasyon Örgütü'nün ("ISO") 27001 ve 27002 standartları, Ulusal Standartlar ve Teknoloji Enstitüsü'nün ("NIST") Siber Güvenlik Çerçevesi veya diğer
benzer standartlar dahil) tutarlı fiziksel, idari ve teknik güvenlik önlemlerini sürdürecektir. Tedarikçi tarafından idame ettirilen önlemler aşağıda Madde 4.1 – 4.18'de açıklanan asgari gereklilikleri içerecektir.

4.1 **Yazılı Bilgi Güvenliği Programı**. Tedarikçi: (a) bu Güvenlik Politikasında belirtilen gereklilikleri karşılayan uygun politikaları, prosedürleri ve standartları içeren; (b) güvenlik sorunlarının (Güvenlik Olayları dahil) iletilmesinden ve yönetilmesinden sorumlu olan bir güvenlik iletişim kişisi belirleyen; (c) en az yılda bir kez gözden geçirilen ve gerektiğinde güncellenen ve (d) Personel için geçerli olan bir yazılı bilgi güvenliği programına sahip olacaktır. Tedarikçi, bilgi güvenliği programını izleyip uygulayacak ve ihlalleri giderecektir.

4.2 **Yama Yönetimi**. Tedarikçi, Kapsama Dahil Olan Bilgi Sistemlerini en son yükseltme, güncelleme, hata düzeltmeleri ve yeni sürümlerle güncel tutacaktır. Tedarikçi, yamasız varlıklar için hafifletici tedbirler uygulayacaktır.

4.3 **Günlük Kaydı**. Tedarikçi, (a) Amazon'un hesaplarının veya bir İzin Verilen Amaç doğrultusunda Tedarikçiye sağlanan kimlik bilgilerinin tüm kullanımları (hem yetkili hem yetkisiz) hakkında günlük verileri ve (b) Amazon

Aşağıdaki çeviri yalnız bilgilendirme amacıyla sağlanmıştır. Bu çeviri ile son güncellenmiş İngilizce sürüm arasında (çeviri gecikmelerine bağlı olanlar dâhil olmak üzere) uyuşmazlık, tutarsızlık veya çelişki olması durumunda İngilizce sürüm geçerli olacaktır.

Bilgilerine veya Kapsama Dahil Olan Bilgi Sistemlerine erişimi olan Amazon personelinin veya Personelin herhangi bir şekilde taklit edilmesi veya taklit edilmeye çalışılması konusunda günlük verileri dahil olmak üzere denetim, olay ve güvenlik günlüklerini toplayacak, yönetecek ve saklayacaktır. Söz konusu günlükler, kaydedilen her olayla ilgili olarak: (i) Olayı başlatan Personel veya hesap, (ii) olayın zamanı ve (iii) etkilenen sistem, veri veya diğer kaynağı tanımlamaya yeterli verileri içerecektir. Tedarikçi, yetkisiz faaliyeti tespit etmeye, araştırmaya ve kurtarmaya yardımcı olmak üzere söz konusu günlükleri düzenli olarak analiz edecektir.

4.4 **Kötü Amaçlı Yazılım Savunmaları**. Tedarikçi, (a) tüm Kapsama Dahil Olan Bilgi Sistemlerine kötü amaçlı yazılımdan koruma yazılımı veya eşdeğer bir güvenlik kontrolü dağıtacak; (b) kötü amaçlı yazılımdan koruma yazılımının veya eşdeğer güvenlik kontrolünün güncelleme, imza ve yapılandırmalarını koruyacak ve (c) kötü amaçlı veya yetkisiz kodların yüklenmesini, yayılmasını ve uygulanmasını tespit etmek, önlemek ve düzeltmek için sistemleri yapılandıracaktır.

4.5 **Risk Yönetimi Programı.** Tedarikçi, risk analizi, riskin ele alınması, risk kabulü ve istisnalar için süreçleri tanımlayan yazılı bir bilgi güvenliği risk yönetimi programına sahip olacaktır.

4.6 **Güvenlik Farkındalığı Eğitimi**. Tedarikçi, işe alım üzerine ve ardından en az yılda bir kez Personele bilgi güvenliği ve veri gizliliği konusunda eğitim sağlayacaktır. Tedarikçi, ayrıca Personelin Tedarikçinin güvenlik ve veri gizliliği politikalarındaki güncellemeler hakkında zamanında bilgilendirilmesini sağlayacaktır.

4.7 **Veri Envanteri**. Tedarikçi, (a) hangi Amazon Bilgilerini İşlemekte olduğu ve (b) Amazon Bilgilerinin nasıl ve nerede İşlendiği ile ilgili bilgileri (örneğin, güncel bir mimari diyagramda) belgeleyecek ve tutacaktır. Tedarikçi, Amazon'un talebi üzerine bu bilgileri Amazon'a sağlayacaktır.

4.8 **Güvenlik Testi.**

4.8.1 Tedarikçi, bu Güvenlik Politikasının gerekliliklerini karşıladığından emin olmak amacıyla yıllık testler gerçekleştirecektir.

4.8.2 Tedarikçi, Tedarikçinin güvenlik savunmalarına sızma testini en az yılda bir kez gerçekleştirecektir. Sızma testi aşağıdakileri içerecektir: (a) Tedarikçinin ağının içinden ve dışından test, (b) sosyal mühendislik (örneğin, kimlik avı simülasyonları) ve (c) kablosuz ağlar için güvenlik testi. Tedarikçi, güvenlik açığı yönetim programının bir parçası olarak belirlenen güvenlik açıklarını giderecektir. Tedarikçi, Amazon'un talebi üzerine Amazon'a söz konusu sızma testi ve güvenlik açığı düzeltmesinin sonuçlarını sağlayacaktır.

4.9 **Ağ Güvenliği**. Tedarikçi, özellikle dış ağlardan yetkisiz ağ erişimini kısıtlayarak tüm Kapsama Dahil Olan Bilgi Sistemlerini koruyacaktır. Tedarikçi, sistemleri yetkisiz erişime karşı korumak amacıyla güvenlik duvarlarını veya diğer eşdeğer güvenlik kontrollerini idame ettirecek ve yapılandıracak ve tüm kurallar için geçerli, belgelenmiş iş vakalarının mevcut olduğundan emin olmak üzere güvenlik duvarı kural kümelerini en az yılda bir kez gözden geçirecektir.

4.10 **Uygun Ortam**. Tedarikçi, Amazon Bilgilerini yalnızca amacına uygun bir ortamda İşleyecek ve Sözleşme kapsamında izin verilmediği sürece Amazon Bilgilerini bir test ortamında İşlemeyecektir.

4.11 **Şifreleme**. Tedarikçi, sektördeki en iyi uygulamalara uygun olarak, beklemedeki ve harici ağlar arasında geçiş halindeki tüm Amazon Bilgilerini şifreleyecektir. Amazon Bilgilerinin dahili Tedarikçi ağlarında iletilmesi halinde, bunlar sektördeki en iyi uygulamaları karşılayan şifreli bir protokol aracılığıyla iletilecektir. Tedarikçi, şifreleme anahtarlarını sektördeki en iyi uygulamalara uygun olarak yönetip güvence altına alacaktır.

4.12 **İdari Ayrıcalıkların Kontrollü Kullanımı**. Tedarikçi, idari işlevleri NIST Siber Güvenlik Çerçevesi veya ISO 27002 uyarınca yönetecektir. Tedarikçi, en azından idari hesapları standart hesaplardan ayıracak ve idari hesapları, yalnızca idari işlevleri gerçekleştirmek için gerekli olan yeteneklerle sınırlayacaktır. Tedarikçi, tüm idari hesap işlemlerini bireysel bir kullanıcıya atfedilebilecek şekilde kaydedecektir. Standart bir hesaba sağlanan idari

Aşağıdaki çeviri yalnız bilgilendirme amacıyla sağlanmıştır. Bu çeviri ile son güncellenmiş İngilizce sürüm arasında (çeviri gecikmelerine bağlı olanlar dâhil olmak üzere) uyuşmazlık, tutarsızlık veya çelişki olması durumunda İngilizce sürüm geçerli olacaktır.

kabiliyetler en az ayrıcalıklı nitelikte olacak ve bireysel bir kullanıcıya atfedilebilecek şekilde günlüğe kaydedilecektir.

4.13 **Erişim Kontrolü.**

4.13.1 **Benzersiz Kimlikler**. Tedarikçi, idari erişime sahip hesaplar dahil olmak üzere Amazon Bilgileri veya Kapsama Dahil Olan Bilgi Sistemlerine erişimi olan Personele bireysel, benzersiz kimlikler atayacaktır.

4.13.2 **Yalnızca "Bilmesi Gerekenler"**. Tedarikçi, Amazon Bilgilerine ve Kapsama Dahil Olan Bilgi Sistemlerine erişimi yalnızca İzin Verilen Amaç doğrultusunda "bilmesi gereken" Personelle sınırlayacaktır.

4.13.3 **Kullanıcı Erişimi İncelemesi**. Tedarikçi, en az 90 günde bir, Amazon Bilgileri ve Kapsama Dahil Olan Bilgi Sistemlerine erişimi olan Personel ve hizmetlerin listesini inceleyecek ve artık erişimi gerektirmeyen hesaplardan erişimi kaldıracaktır.

4.13.4 **Çoklu Oturum Açma (SSO).** Amazon personel kimlik doğrulaması gerektiren tüm Tedarikçi hizmetleri, söz konusu kimlik doğrulamasını sağlamak için bir Amazon kimlik sağlayıcısı (örneğin, Amazon Federate) ile entegre olmalıdır. Söz konusu hizmetler, kimlik doğrulama için Tedarikçi tarafından sağlanan veya Tedarikçi tarafından yönetilen kimlik bilgilerini kullanmamalıdır.

4.14 **Parola Yönetimi.**

4.14.1 **Güçlü Parolalar**. Tedarikçi, üretici tarafından sağlanan varsayılanları hiçbir Kapsama Dahil Olan Bilgi Sisteminde sistem parolaları ve diğer güvenlik parametreleri için kullanmayacaktır. Tedarikçi, tüm Kapsama Dahil Olan Bilgi Sistemlerinde NIST SP 800-63B'de açıklanan en iyi uygulamalara uygun şekilde sistem tarafından zorunlu tutulan "güçlü şifreler" kullanılmasını zorunlu kılacak ve bunların kullanılmasını sağlayacaktır. Tedarikçi, tüm parolaların ve erişim bilgilerinin gizli tutulmasını ve Personel arasında paylaşılmamasını zorunlu tutacaktır.

4.14.2 **Kilitleme**. Tedarikçi, bir hesap art arda ondan (10) fazla yanlış parola denemesi yaptığında Amazon Bilgilerine veya Kapsama Dahil Olan Bilgi Sistemlerine erişimi olan hesapları devre dışı bırakan "hesap kilitleme" işlemi idame ettirecek ve bunu zorunlu tutacaktır.

4.15 **Uzaktan Erişim; Çok Faktörlü Kimlik Doğrulama**. Tedarikçi, herhangi bir Tedarikçi ağı, sistemi, uygulaması veya başka bir varlığa uzaktan erişim için çok faktörlü kimlik doğrulama (başka bir deyişle, bir kullanıcının kimliğini doğrulamak için en az iki faktör gerektiren doğrulama) uygulayacaktır.

4.16 **"Toplu Olarak" Erişim**. Bu bölümün amaçları için, "toplu olarak" erişim, veri tabanı sorgusu, rapor oluşturma veya diğer toplu veri aktarımı yolları ile verilere erişmek demektir.

4.16.1 Sözleşmede açıkça belirtilmediği veya Amazon tarafından yazılı olarak aksi belirtilmediği sürece, Amazon Bilgileri ister Amazon veya Tedarikçi tarafından kontrol edilen bir veri tabanında olsun, ister dosya tabanlı arşivlerde (örneğin, düz dosyalar) depolama dahil olmak üzere başka bir yöntem kullanılarak depolanmış olsun Tedarikçi, Amazon Bilgilerine "toplu olarak" erişmeyecek ve erişime izin vermeyecektir; .

4.16.2 Amazon'un "toplu olarak" erişime izin verdiği hallerde, Tedarikçi: (a) söz konusu erişimi yalnızca "bilmesi gereken" belirli Personel ile sınırlayacak ve (b) söz konusu erişimin Madde 4.3'ün gerekliliklerine uygun şekilde açık şekilde yetkilendirilmesini ve günlüğe kaydedilmesini gerekli kılacaktır. Amazon'un,
Madde 10 güvenlik incelemeleri veya Madde 11 Güvenlik Olayları ile koordinasyon halinde talebi üzerine, Tedarikçi bu madde belirtilen "toplu olarak" erişime ilişkin tüm günlükleri Amazon'a sağlayacaktır.

4.17 Veri Ayırma. Tedarikçi, Amazon Bilgilerini her zaman Tedarikçi ve herhangi bir üçüncü tarafın bilgilerinden fiziksel veya mantıksal olarak ayıracaktır. Tedarikçi, ayırma mümkün değilse Amazon Bilgilerinin kayıt, silme ve olay müdahalesi amaçları doğrultusunda diğer bilgilerden ayırt edilebilir olmasını sağlayacaktır.

Aşağıdaki çeviri yalnız bilgilendirme amacıyla sağlanmıştır. Bu çeviri ile son güncellenmiş İngilizce sürüm arasında (çeviri gecikmelerine bağlı olanlar dâhil olmak üzere) uyuşmazlık, tutarsızlık veya çelişki olması durumunda İngilizce sürüm geçerli olacaktır.

4.18 **Tedarikçi Personeli Güvenliği.**

4.18.1 Tedarikçi, Amazon Bilgilerine erişim izni verilen Personelin bu bilgilerin gizliliğini korumasını ve yalnızca İzin Verilen Amaç doğrultusunda kullanmasını sağlamak için tüm makul önlemleri alacaktır. Bu önlemler, bir ifşa etme yasağı sözleşmesi veya Tedarikçi politikası yoluyla gizlilik gerekliliklerinin uygulanmasını içermelidir.

4.18.2 Tedarikçi, (a) Amazon Tarafından Yönetilen Bilgi Sistemine artık erişmeye ihtiyaç duymayan veya (b) artık Tedarikçi Personeli niteliğine sahip olmayan herhangi bir Personel için Amazon Bilgilerine ve Kapsama Dahil Olan Bilgi Sistemlerine erişimi 24 saat içinde sonlandıracaktır. Tedarikçi, herhangi bir Personelin (a) veya (b) gerçekleştikten sonra Amazon Bilgileri veya Kapsama Dahil Olan Bilgi Sistemlerine erişimi 24 saatten uzun bir süre elde tutması durumunda Tedarikçinin bundan haberdar olmasından sonraki 24 saat içinde security@amazon.com adresine e-posta göndererek Amazon'u bu süren erişim hakkında bilgilendirecektir.

5. **ÖDEME GÜVENLİĞİ GEREKLİLİKLERİ**. Tedarikçinin ödeme kart sahibi verilerine erişimi varsa veya İşleyecekse Tedarikçi Ödeme Kartı Sektörü Veri Güvenliği Standardının (PCI DSS) en son sürümüne uyacaktır.

6. **ALT YÜKLENİCİLER.**

6.1 Tedarikçi, Amazon'un ön yazılı onayı olmaksızın bu Güvenlik Politikası kapsamındaki yükümlülüklerinin hiçbirini herhangi bir üçüncü tarafa (toplu olarak "Alt Yükleniciler") alt sözleşme ile vermeyecek veya devretmeyecektir. Herhangi bir alt sözleşmenin veya yetki devrinin varlığına veya koşullarına bakılmaksızın Tedarikçi bu Güvenlik Politikası kapsamındaki yükümlülüklerinin tam olarak yerine getirilmesinden sorumlu olmaya devam edecektir. Bu Güvenlik Politikasının hükümleri ve koşulları Tedarikçinin Alt Yüklenicileri ve Alt yüklenicilerin Personeli için bağlayıcı olacaktır.

6.2 Tedarikçi herhangi bir Alt Yüklenici Kapsama Dahil Olan Bilgi Sistemi kullanırsa Tedarikçi, Alt Yüklenici Kapsama Dahil Olan Bilgi Sistemlerinin ve güvenlik kontrollerinin bir güvenlik incelemesini yapacak ve Amazon'un talebi üzerine, Amazon'un talep ettiği formatta Alt Yüklenici Kapsama Dahil Olan Bilgi Sistemlerinin güvenlik kontrolleri hakkında Amazon'a periyodik bildirimde bulunacaktır (örneğin, Tasdik Hizmetlerine İlişkin Standartlar Hakkında Beyan No.16 (SSAE 16)).

7. AMAZON TARAFINDAN YÖNETİLEN BİLGİ SİSTEMLERİNE ERİŞİM. Amazon, Tedarikçiye Amazon Bilgilerini web portalları veya diğer halka açık olmayan internet siteleri veya dış ağlar (her biri bir "Amazon Tarafından Yönetilen Bilgi Sistemi") aracılığıyla yalnızca İzin Verilen Amaç doğrultusunda İşleme hakkı verebilir. Amazon, Tedarikçinin Amazon Tarafından Yönetilen Bilgi Sistemini kullanarak herhangi bir Amazon Bilgisini İşlemesine izin verirse Tedarikçi ve Personeli aşağıdaki gerekliliklere uymalıdır:

7.1 **Hesaplar**. Tedarikçi, Tedarikçi Personelinin yalnızca Amazon'un her bir kişi için belirlediği Amazon Tarafından Yönetilen Bilgi Sistemi hesabını kullanmasını sağlayacak ve Tedarikçi Personelinin erişim bilgilerini gizli tutmasını ve bunları paylaşmamasını talep edecektir.

7.2 **Sistemler.** Tedarikçi ve Personeli, Amazon Tarafından Yönetilen Bilgi Sistemlerini yalnızca (a) Tedarikçi tarafından yönetilen ve tam disk şifreleme kullanan işletim sistemlerini çalıştıran ve (b) Bölüm 4.2 (Yama yönetimi), 4.4 (Kötü Amaçlı Yazılım savunmaları) ve 4.9 (Ağ güvenliği) gerekliliklerini karşılayan bilişim veya işleme sistemleri veya uygulamaları aracılığıyla kullanacaktır.

7.3 **Kısıtlamalar**. Tedarikçi ve Personeli, Amazon tarafından ön yazılı olarak onay verilmedikçe herhangi bir Amazon Bilgi Sisteminden herhangi bir Amazon Bilgisini herhangi bir ortamda indirmeyecek, yansıtmayacak veya kalıcı olarak saklamayacaktır.

7.4 **Hesap Sonlandırma**. (a) Amazon Tarafından Yönetilen Bilgi Sistemine artık erişmeye ihtiyaç duymayan veya (b) artık Tedarikçi Personeli niteliğine sahip olmayan (örneğin, söz konusu kişinin artık Tedarikçi tarafından istihdam

edilmemesi) herhangi bir Personel için Tedarikçi, söz konusu Personelin Amazon Tarafından Yönetilen Bilgi Sistemine erişimini derhal (en fazla 24 saat içinde) sonlandıracak veya Amazon'a söz konusu erişimi kaldırması için bildirimde bulunacaktır.

8. **AMAZON ETKİ ALANLARI VEYA URL'LERİ.** Tedarikçinin Amazon'un tek başına kullanımı için sağladığı herhangi bir etki alanı veya URL, Sözleşmenin feshinden sonra en az 5 yıl boyunca Tedarikçi tarafından herhangi bir üçüncü tarafa verilmemeli veya yeniden kullanılmamalıdır.

9. VERİ İADESİ VE SİLME; ADLİ ORTAM İMHASI.

9.1 **Veri İadesi ve Silme**. Amazon'un talebi üzerine, Tedarikçi, Amazon'un iade ve/veya silme isteyen bildirimine uygun şekilde tüm Amazon Bilgilerini hemen (ama en çok 72 saat içinde) Amazon'a iade edecek ve kalıcı ve güvenli şekilde silecektir. Tedarikçi ayrıca Amazon Bilgilerinin tüm canlı (çevrim içi veya ağ üzerinden erişilebilir olan) örneklerini, İzin Verilen Amacın tamamlanması, bu Sözleşmenin feshi veya sona ermesinden hangisi daha erken ise, o tarihten sonra 30 gün içinde kalıcı ve güvenli şekilde silecektir. Amazon tarafından talep edilmesi halinde Tedarikçi tüm Amazon Bilgilerinin silinmiş olduğunu yazılı olarak tasdik edecektir. Açıklık getirmek için, bu bölüm, Bölüm 9.3 uyarınca Arşiv Kopyaları için geçerli olmayacaktır.

9.2 **Veri Temizleme**. Tedarikçi tarafından silinen tüm Amazon Bilgileri, ilgili cihaz türünün temizlenmesi için NIST SP 800-88 Revizyon 1, Ortam Temizleme Yönergeleri'nde (18 Aralık 2014, Ek A) yer alan Asgari Temizleme Önerileri uyarınca silinecektir. Tedarikçi, ilgili cihaz türü için NIST SP 800-88'de rehberlik olmaması halinde, Amazon Bilgilerini içeren cihazı aşağıdaki yollardan biriyle imha edecektir: (a) NIST SP 800-88'de tanımlandığı gibi temizleme, (b) NIST SP 800-88'de tanımlandığı gibi imha etme veya (c) Amazon Bilgilerinin sınıflandırılması ve hassasiyetine dayalı olarak Amazon'un gerekli tutabileceği diğer standartlar.

9.3 **Arşiv Kopyaları**. Tedarikçinin Amazon Bilgilerinin arşiv kopyalarını yasal olarak saklaması gerekirse Tedarikçi arşivlenmiş Amazon Bilgilerini başka bir amaç doğrultusunda kullanmayacaktır ve bu Güvenlik Politikası kapsamındaki tüm yükümlülüklere bağlı kalacaktır. Arşivlenen tüm Amazon Bilgileri şifrelenmeli ve şifrelenmiş Amazon Bilgilerini barındıran veya saklayan Kapsama Dahil Olan Bilgi Sisteminin şifreleme için kullanılan anahtarların bir kopyasına erişiminin olmadığı yerlerde saklanmalıdır. Herhangi bir çevrim dışı veya "soğuk" (başka bir deyişle, anında veya etkileşimli kullanıma açık olmayan) yedekleme, fiziksel olarak güvenli bir tesiste saklanmalıdır.

9.4 **Adli Ortam İmhası**. Amazon Bilgilerini içermekte olan veya herhangi bir zamanda içermiş olan herhangi bir donanım, yazılım veya başka bir ortamı herhangi bir zamanda imha etmeden önce, Tedarikçi NIST SP 800-88, Ek A'ya uygun olarak donanım, yazılım veya başka bir ortamın adli olarak tam imhasını gerçekleştirecektir. Bu imha gerekliliği, Tedarikçinin fiziksel erişimi veya kontrolü olmayan depolama ortamları için geçerli olmayacaktır. Söz konusu durumlarda Tedarikçi, sektördeki en iyi uygulamaları takip etmek suretiyle artık ihtiyaç duyulmadığında Amazon Bilgilerinin güvenli bir şekilde silinmesini sağlayacaktır.

> 9.4.1 Tedarikçi, Amazon'dan ön açık yazılı onay almadığı sürece, bu Bölüm uyarınca adli olarak imha edilmedikçe Amazon Bilgilerini herhangi bir zamanda içeren herhangi bir donanım, yazılım veya diğer ortamı satmayacak, yeniden satmayacak, bağışlamayacak, yenilemeyecek veya başka bir şekilde devretmeyecektir.

10. **GÜVENLİK İNCELEMELERİ**. Amazon'un talebi üzerine, Tedarikçi: (a) bir Amazon risk değerlendirmesini tamamlayacak, (b) Tedarikçinin bu Güvenlik Politikasına uyumunu doğrulamak için Amazon tarafından talep edilen kanıtları sağlayacak, (c) Amazon'un veya onun adına atanan üçüncü bir tarafın Tedarikçinin bu Güvenlik Politikasına uyumunu incelemesine izin verecek ve/veya (d) Madde 4.3'te atıfta bulunulan tüm günlükleri Açık Siber Güvenlik Şema Çerçevesi (OCSF) formatında Amazon'a sağlayacaktır. Tedarikçi, Amazon'un uzaktan incelemesi için bu tür kanıtları sağlamak yerine herhangi bir kanıtın şahsen veya yerinde bir denetimle incelenmesini talep ederse Tedarikçi söz konusu sahada denetimle ilgili seyahat maliyetini ve diğer masrafları karşılayacaktır. Tedarikçi,

Aşağıdaki çeviri yalnız bilgilendirme amacıyla sağlanmıştır. Bu çeviri ile son güncellenmiş İngilizce sürüm arasında (çeviri gecikmelerine bağlı olanlar dâhil olmak üzere) uyuşmazlık, tutarsızlık veya çelişki olması durumunda İngilizce sürüm geçerli olacaktır.

herhangi bir değerlendirme veya incelemede herhangi bir bulgu tespit edilirse masrafları münhasıran Tedarikçiye ait olmak üzere, bu bulguları Amazon'u makul şekilde memnun edecek şekilde ve üzerinde mutabakata varılmış bir zaman dilimi içinde düzeltmek için gerekli tüm makul önlemleri hemen alacaktır.

11. **GÜVENLİK OLAYLARI.**

11.1 **Güvenlik Olayı Bildirimi**. Tedarikçi, Amazon Bilgilerine veya Kapsama Dahil Olan Bilgi Sistemine yetkisiz erişim, toplanma, edinilme, kullanılma, iletilme, açıklanma, bozulma veya kaybı öğrendikten veya makul olarak buna inandıktan sonra en geç 24 saat içinde olmak üzere Amazon'u mümkün olan en kısa sürede bilgilendirecektir ("Güvenlik Olayı"). Tedarikçi, Güvenlik Olayı bildirimlerini security@amazon.com adresine gönderecektir.

11.2 **Olay Müdahale Planı**. Tedarikçi yazılı bir olay müdahale planı tutacak ve talep üzerine bunun bir kopyasını Amazon'a sağlayacaktır. Tedarikçi, her Güvenlik Olayını Tedarikçinin yazılı olay müdahale planını ve sektördeki en iyi uygulamaları takip ederek zamanında düzeltecektir. Tedarikçi, planı en az yılda bir kez gözden geçirecek, test edecek ve (gerekirse) güncelleyecektir.

11.3 **Amazon ile İş Birliği**. Tedarikçi (a) Amazon'un Güvenlik Olayını soruşturmasına yardımcı olacak; (b) Personel ve Güvenlik Olayına veya müdahalesine katılan diğer kişiler ile görüşmeleri kolaylaştıracak; (c) Tedarikçinin Güvenlik Olayı soruşturma ve müdahalesinin yazılı ayrıntılarını tutacak ve (d) Amazon tarafından talep edilen tüm ilgili kayıt, günlük, dosya, veri raporlama, adli raporlar, soruşturma raporları ve diğer materyalleri Amazon'a sağlayacaktır.

11.4 **Üçüncü Taraf Bildirimleri**. Tedarikçi, yasada aksi öngörülmedikçe (a) herhangi bir Güvenlik Olayı hakkında herhangi bir üçüncü tarafa (herhangi bir düzenleyici makam veya müşteri dahil) bildirimde bulunmadan veya (b) herhangi bir Güvenlik Olayı ile ilgili herhangi bir bildirimde veya kamu açıklamasında Amazon'un kimliğini belirtmeden önce Amazon'un ön yazılı onayını alacaktır. Amazon, yasada aksi öngörülmedikçe bir Güvenlik Olayı bildiriminin herhangi bir üçüncü tarafa sağlanıp sağlanmayacağını ve bu bildirimin biçimini, zamanlamasını ve içeriğini belirleme hakkına sahip olacaktır.

12. **YASAL SÜREÇ BİLDİRİMİ**. Yasal süreç bildirimi. Yasa ile yasaklanan haller dışında, yasal sürece veya diğer geçerli yasaya yanıt olarak Amazon Bilgileri gerekiyorsa Tedarikçi, Amazon'un koruyucu bir hüküm veya başka uygun bir hukuk yolu aramasını sağlamak için Amazon'a yeterli bildirimde bulunacaktır.

13. **TANIMLAR**.

13.1"**Sözleşme**", bu Güvenlik Politikasına atıfta bulunan herhangi bir sözleşme demektir.

13.2 "**Amazon**", Amazon.com, Inc. ve bağlı kuruluşları demektir.

13.3 "**Amazon Bilgileri**", (a) tüm Amazon Gizli Bilgileri (taraflar arasındaki herhangi bir başka sözleşmede tanımlandığı şekilde); (b) Tedarikçi veya bağlı kuruluşları tarafından, Amazon adına veya Amazon'dan veya başka bir şekilde Sözleşme ile bağlantılı olarak edinilen, erişilen, toplanan, alınan, saklanan veya muhafaza edilen herhangi bir biçimdeki tüm veri, kayıt, dosya, içerik veya bilgiler; ve Anonimleştirilmiş olsalar bile (c) (a) veya (b)'den türetilen bilgiler demektir.

13.4 "**Anonimleştirme**", Amazon'a veya herhangi bir kullanıcı, cihaz tanımlayıcısı, kaynak, ürün, hizmet, bağlam veya markaya ait herhangi bir veriyi veya bilgiyi (Amazon Bilgileri dahil) tanımlamayan, tanımlanmasına izin vermeyen ve başka bir şekilde Amazon'a atfedilemeyen bir şekilde veya biçimde İşlemek demektir.

13.5 "**Kapsama Dahil Olan Bilgi Sistemleri**", Tedarikçinin Amazon Bilgilerini İşlemek için kullandığı herhangi bir sistem demektir.

Aşağıdaki çeviri yalnız bilgilendirme amacıyla sağlanmıştır. Bu çeviri ile son güncellenmiş İngilizce sürüm arasında (çeviri gecikmelerine bağlı olanlar dâhil olmak üzere) uyuşmazlık, tutarsızlık veya çelişki olması durumunda İngilizce sürüm geçerli olacaktır.

13.6 “**Personel”,** Tedarikçi veya Alt yüklenicinin çalışanları, temsilcileri, Alt yüklenicileri ve sistemleri ve ağ kaynaklarının diğer yetkili kullanıcıları anlamına gelir.

13.7 “**İşleme**”, erişim, kullanım, toplama, alma, saklama, değiştirme, iletme, yayma veya başka bir şekilde kullanıma sunma, silme veya imha etme gibi veriler üzerinde herhangi bir işlem yapmak demektir.

13.8 “**Tedarikçi**”, bir Sözleşmede tanımlanan her tedarikçi, satıcı veya yüklenici ve bir Sözleşmeye tabi olan diğer herhangi bir sağlayıcı demektir.