Aşağıdaki çeviri yalnızca bilgilendirme amaçları için sağlanmıştır. Bu çeviri ve İngilizce sürümü arasında farklılık, tutarsızlık veya uyuşmazlık bulunması halinde (özellikle çeviri gecikmeleri yüzünden) İngilizce sürümü geçerli olacaktır.

TEDARİKÇİ GÜVENLİK POLİTİKASI

Son güncelleme tarihi: 28 Ocak 2022

1. KAPSAM; TANIMLAR.

1.1 Güvenlik Politikası. Tedarikçi, Amazon'un bu politikada belirtilen bilgi güvenliği gerekliliklerine ("**Güvenlik Politikası**") her bakımdan uyacaktır. Bu Güvenlik Politikası, Tedarikçinin Sözleşme kapsamındaki performansı ve Tedarikçinin Amazon Bilgilerine her türlü erişimi, onları toplaması, kullanması, depolaması, iletmesi, açıklaması, imha etmesi veya silmesi ve bunlar hakkındaki güvenlik vakaları için geçerlidir. Bu Güvenlik Politikası, Amazon ile yapılan diğer tüm sözleşmeler veya Tedarikçi için geçerli olan diğer tüm yasalar, Tedarikçinin Amazon ile yapılan diğer tüm sözleşmeler, Amazon Bilgileri veya İzin Verilen Amaç kapsamındaki performansı dâhil olmak üzere Tedarikçinin diğer yükümlülüklerinin hiçbirini sınırlandırmaz. Bu Güvenlik Politikasının taraflar arasındaki herhangi bir açıklamama sözleşmesi veya taraflar için geçerli olan diğer herhangi bir sözleşme ile çelişmesi halinde, Tedarikçi, daha az koruyucu olan gerekliliklerin daha çok koruyucu olan gerekliliklerden üstün olduğu açıkça belirtilmediği sürece (bu Amazon tarafından belirlenebilir), çelişkiyi hemen Amazon'a bildirecek ve Amazon Bilgileri için daha koruyucu olan gerekliliklere uyacaktır. Amazon zaman zaman yalnız kendi takdirine bağlı olarak bu Güvenlik Politikasını değiştirebilir ancak bu değişikliklerin ticari bakımdan makul olmaması halinde Amazon talep üzerine görüşerek uygun ek ücretler üzerinde anlaşmaya varacaktır.

1.2 Tanımlar.

1.2.1 "**Toplu Duruma Getirmek**", Amazon Bilgilerini Tedarikçinin veya herhangi bir üçüncü tarafın verileri veya bilgileri ile birleştirmek veya depolamak demektir.

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

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

1.2.4 "**Anonimleştirmek**", herhangi bir veriyi veya bilgiyi (Amazon Bilgileri dâhil) Amazon'u veya herhangi bir kullanıcıyı, cihaz tanımlayıcıyı, kaynağı, ürünü, hizmeti, içeriği veya markasını tanımlamayan, tanımlamaya izin vermeyen ve başka bir şekilde bunlara atfedilemeyen şekilde kullanmak, toplamak, depolamak, iletmek veya dönüştürmek demektir.

1.2.5 "**Amazon Bilgileri**", münferit ve toplu şekilde şu demektir: (a) tüm Amazon Gizli Bilgileri (bir açıklamama sözleşmesinde veya taraflar arasındaki diğer sözleşmelerde tanımlanan şekilde); (b) Tedarikçi veya bağlı kuruluşları tarafından Amazon'dan veya onun adına veya bu Güvenlik Politikası veya hizmetler veya tarafların Sözleşme kapsamında veya Sözleşme ile ilişkili şekilde hakları ifası veya kullanması ile bağlantılı olarak elde edilen, erişim sağlanan, toplanan, teslim alınan, depolanana veya muhafaza edilen herhangi bir biçimdeki veya biçim içindeki diğer tüm veriler, kayıtlar, dosyalar, içerik veya bilgiler ve (c) Anonimleştirilse bile (a) veya (b)'den elde edilen bilgiler.

1.2.6 "Tedarikçi", bir Sözleşmede tanımlanan her Tedarikçi, Satıcı veya Yüklenici ve bir Sözleşmeye tabi olan diğer herhangi bir sağlayıcı demektir.

1.3 İzin Verilen Amaç. Tedarikçi, yalnızca Sözleşme kapsamında açıkça izin verilen Amazon Bilgilerine ve yalnızca Sözleşme kapsamında ürünler veya hizmetler sağlamak amacı ile bu Güvenlik Politikası kapsamında verilen lisanslar ile (var ise) tutarlı şekilde erişebilir, onları toplayabilir, kullanabilir, depolayabilir ve iletebilir ("**İzin Verilen Amaç**"). Sözleşme kapsamında açıkça yetkilendirilmedikçe Tedarikçi herhangi bir Amazon Bilgisine erişmeyecek, onları toplamayacak, kullanmayacak, depolamayacak veya iletmeyecek ve Anonimleştirilse bile Amazon Bilgilerini Toplu Duruma getirmeyecektir. Amazon'un önceden açık yazılı onayı dışında, Tedarikçi Anonimleştirilse

bile (a) Amazon Bilgilerini herhangi bir üçüncü tarafa aktarmayacak, kiralamayacak, takas etmeyecek, ticaretini yapmayacak, satmayacak, ödünç vermeyecek veya kiralık vermeyecek veya başka bir şekilde dağıtmayacak veya sağlamayacaktır veya (b) Anonimleştirilse bile Amazon Bilgilerini başka herhangi bir bilgi veya veri ile Toplu Duruma getirmeyecektir.

2. AMAZON GÜVENLİK POLİTİKASI.

2.1 Temel Güvenlik Gereklilikleri. Tedarikçi, Amazon Bilgilerinin sınıflandırılması ve hassasiyeti temelinde mevcut en iyi endüstri standartları ve Amazon tarafından belirtilen diğer gereklilikler ile tutarlı şekilde, (a) Tedarikçi tarafından erişilen, toplanan, kullanılan, depolanan veya iletilen Amazon Bilgilerinin güvenliğini ve gizliliğini korumak ve (b) bu bilgileri onların güvenliğine ve bütünlüğüne karşı bilinen veya makul olarak beklenen tehditlere veya tehlikelere, kaza sonucu kaybolmaya, değiştirilmeye ve açıklanmaya ve diğer tüm yasa dışı işleme şekillerine karşı korumak için fiziksel, idari ve teknik önlemleri ve diğer güvenlik önlemlerini alacaktır. Sınırlandırma olmaksızın, Tedarikçi, Amazon Bilgilerini işlemek için kullandığı veya Amazon Bilgilerine erişimi olan tüm sistemler için aşağıdaki gerekliliklere uyacaktır ("**Amazon Bilgi Sistemleri**"):

2.1.1 Ağ Güvenliği. Tedarikçi, özellikle dış İnternetten olan yetkisiz ağ erişimini kısıtlayarak tüm Amazon Bilgi Sistemlerini koruyacaktır. Tedarikçi, Amazon Bilgilerini her zaman korumak için bir güvenlik duvarı gibi etkili bir ağ güvenlik çözümü kuracak ve bunu sürdürecektir.

2.1.2 Güncellemeler. Ulusal Standartlar ve Teknoloji Enstitüsü ("NIST") Özel Yayını ("SP") 800-40 Revizyon 3'te belirtildiği gibi, Tedarikçi, Amazon Bilgi Sistemlerini en son yükseltmeler, güncellemeler, hata düzeltmeleri ve yeni sürümler ve Amazon Bilgilerinin güvenliğini sağlamak için gerekli olan diğer tüm değişiklikler ile güncel durumda tutacaktır.

2.1.3 Kötü amaçlı yazılımdan koruma. Tedarikçi, kötü amaçlı yazılımların tehlike yaratması ve yayılması riskini azaltmak için her zaman kötü amaçlı yazılımdan koruma yazılımı veya eşdeğer bir güvenlik kontrolü kullanacaktır. Kullanılması halinde, Tedarikçi kötü amaçlı yazılımdan koruma yazılımını güncel durumda tutacaktır.

2.1.4 Şifreleme. Tedarikçi, hareketsiz durumdaki verileri ve açık ağlar üzerinden gönderilen verileri en iyi endüstri uygulamalarına uygun şekilde şifreleyecektir.

2.1.5 Test. Tedarikçi, kendi güvenlik sistemlerinin ve süreçlerinin bu Güvenlik Politikasının veya Tedarikçi ve Amazon tarafından en son kararlaştırılmış güvenlik politikasının gerekliliklerini karşıladığından emin olmak için onları düzenli olarak test edecektir. Bölüm 1.1 uyarınca Güvenlik Politikasında değişiklikler olması durumunda, bu değişiklikler Tedarikçi ile Amazon arasında anlaşmaya varılıncaya kadar (e-posta yeterli olacaktır) bu Bölümün amaçları için yürürlüğe girmeyecektir.

2.1.6 Erişim Kontrolleri. Tedarikçi, aşağıdaki gerekliliklere uymak dâhil olmak üzere Amazon Bilgilerini güvenceye alacaktır:

2.1.6.1 Tedarikçi, Amazon Bilgilerine veya Amazon Bilgi Sistemlerine bilgisayar erişimi olan her kişiye benzersiz bir kimlik atayacaktır.

2.1.6.2 Tedarikçi, Amazon Bilgilerine erişimi yalnızca İzin Verilen Amaç için "bilmesi gereken" kişiler ile kısıtlayacaktır.

2.1.6.3 Tedarikçi, Amazon Bilgilerine erişimi olan kişilerin ve hizmetlerin listesini düzenli olarak inceleyecek ve Amazon Bilgi Sistemlerine erişmesi artık gerekmeyen hesapları kaldıracaktır. Bu inceleme en az 90 günde bir yapılmak zorundadır.

2.1.6.4 Tedarikçi, üretici tarafından sağlanan varsayılanları hiçbir Amazon Bilgi Sisteminde sistem parolaları ve diğer güvenlik parametreleri için kullanmayacaktır. Tedarikçi, tüm Amazon 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 kimlik bilgilerinin gizli tutulmasını ve personel arasında paylaşılmamasını gerekli tutacaktır.

2.1.6.5 Tedarikçi, bir hesap art arda ondan (10) fazla yanlış parola denemesi yaptığında Amazon Bilgilerine veya Amazon Bilgi Sistemlerine erişimi olan hesapları devre dışı bırakan "hesap kilitleme" işlemi bulunduracak ve bunu zorunlu tutacaktır.

2.1.6.6 Amazon tarafından yazılı olarak açıkça yetki verilmesi dışında, Tedarikçi, Amazon Bilgilerini her zaman (saklama, işleme veya aktarma sırasında dâhil) Tedarikçinin ve herhangi bir üçüncü tarafın bilgilerinden fiziksel veya mantıksal olarak ayıracaktır.

2.1.6.7 Amazon tarafından yazılı olarak ek fiziksel erişim kontrolleri istenmesi halinde Tedarikçi bu güvenli fiziksel erişim kontrolü önlemlerini uygulayacak ve kullanacaktır.

2.1.6.8 Tedarikçi, Amazon'un makul talebi üzerine (a) Amazon'un hesaplarının veya İzin Verilen Amaç için Tedarikçiye sağlanan kimlik bilgilerinin (örneğin, sosyal medya hesabı kimlik bilgileri) tüm kullanımları (gerek yetkili gerek yetkisiz) hakkındaki günlük verilerini ve (b) Amazon personelinin veya Amazon Bilgilerine erişimi olan Tedarikçi personelinin herhangi bir şekilde taklit edilmesi veya taklit edilme girişimleri hakkındaki ayrıntılı günlük verilerini Amazon'a sağlayacaktır.

2.1.6.9 Tedarikçi, erişim günlüklerini kötü niyetli davranış veya yetkisiz erişim belirtileri bakımından düzenli olarak inceleyecektir.

2.1.7 Tedarikçinin Politikası. Tedarikçi, politika ihlallerini belirleme ve kaydetme yöntemleri dâhil olmak üzere, çalışanlar, alt yükleniciler, temsilciler ve tedarikçiler için bu Güvenlik Politikasında belirtilen standartları karşılayan bir bilgi ve ağ güvenliği politikası bulunduracak ve uygulayacaktır. Söz konusu ihlallerin bir Güvenlik Vakası (aşağıda tanımlanmıştır) oluşturabileceğine dair gerek Tedarikçinin gerek Amazon'un makul bir şüphesi olması halinde Amazon'un talebi üzerine Tedarikçi Amazon'a Tedarikçinin bilgi ve ağ güvenliği politikasının ihlalleri hakkında bilgi sağlayacaktır.

2.1.8 Alt sözleşme. Tedarikçi, Amazon'un önceden yazılı onayı olmadan bu Güvenlik Politikası kapsamındaki yükümlülüklerinin hiçbirini alt yükleniciye veya temsilciye (topluca "**Alt Yükleniciler**") alt sözleşme ile vermeyecek veya yetkisini teslim etmeyecektir. 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 personeli için bağlayıcı olacaktır. Tedarikçi (a) Alt Yüklenicilerinin ve personelinin bu Güvenlik Politikasına uymasını sağlayacak ve (b) Tedarikçinin Alt Yüklenicilerinin ve personelinin tüm davranışlarından, ihmallerinden, dikkatsizliklerinden ve yanlış davranışlarından sorumlu olacaktır

2.1.9 Uzaktan Erişim. Tedarikçi, Amazon Bilgi Sistemlerine herhangi bir erişimin çok faktörlü kimlik doğrulama gerektirmesini sağlayacaktır (örneğin kullanıcıları tanımlamak için en az iki ayrı faktör gerektirmesi).

2.1.10 "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. Amazon tarafından yazılı olarak açıkça yetki verilmesi dışında, Tedarikçi, Amazon Bilgilerinin Tedarikçi veya Amazon tarafından kontrol edilen bir veri tabanında olup olmadığına veya dosya tabanlı arşivlerde (örneğin düz dosyalarda) depolama dâhil olmak üzere başka herhangi bir şekilde depolanıp depolanmadığına bakılmaksızın Amazon Bilgilerine "toplu olarak" erişmeyecek ve erişilmesine izin vermeyecektir. Özellikle, bu bölüm, İzin Verilen Amaç için gereken şekilde münferit kayıtlara erişim dışında Amazon Bilgilerine tüm erişimi yasaklamaktadır. Tedarikçi, Amazon Bilgilerine "toplu olarak" erişimin denenmesi veya başarılması ile ilgili ayrıntılı günlük verilerini saklayacak ve Tedarikçinin Bölüm 2.5 (Güvenlik İncelemesi) kapsamındaki yükümlülüklerinin bir parçası olarak bu günlüklerden raporlar sağlayacaktır. Amazon, Amazon Bilgilerine "toplu olarak" erişim için Tedarikçiye yazılı yetki verirse Tedarikçi (a) söz konusu erişimi yalnızca "bilmesi gereken" belirli çalışanlar ile sınırlandıracak ve (b) erişimi sınırlayan ve tüm erişimlerin açıkça yetkilendirilmesini ve kaydedilmesini gerektiren araçlar kullanacaktır.

2.1.11 Tedarikçi Personeli. Amazon, Tedarikçi personelinin Amazon Bilgilerine erişimini, şekli Amazon tarafından belirlenmek üzere, onların kişisel açıklamama sözleşmeleri imzalanması ve Amazon'a teslim etmesi koşuluna bağlayabilir. Amazon'un gerekli tutması halinde Tedarikçi personeli kişisel açıklamama sözleşmesi imzalayacaktır. Tedarikçi, Amazon'un bilgilerine erişimi olacak Tedarikçi personelinden imzalanmış kişisel açıklamama sözleşmelerini alacak ve Amazon'un teslim edecektir (Tedarikçi personeline erişim sağlamadan veya bilgi verilmeden önce). Tedarikçi ayrıca Amazon Bilgi Sistemlerindeki

Amazon Bilgilerine erişmiş veya bu bilgileri almış olan tüm Tedarikçi personelinin listesini tutacak ve bu listeyi talep üzerine hemen Amazon'a sağlayacaktır. Tedarikçi, (a) artık Amazon Bilgilerine erişmeye gerek duymayan veya (b) artık Tedarikçi personeli niteliğine sahip olmayan (örneğin, birey Tedarikçinin istihdamından çıkmıştır) herhangi bir Tedarikçi personeli için Amazon Bilgilerine ve Amazon Bilgi Sistemlerine erişimi hemen (en çok 24 saat içinde) sonlandıracaktır. Bu gibi herhangi bir personelin Amazon Bilgi Sistemlerindeki Amazon Bilgilerine erişme yetkisi varsa Tedarikçi 24 saat içinde Amazon'u da bilgilendirecektir.

2.2 Amazon Dış Ağına ve Tedarikçi Portallarına Erişim. Amazon, web portalları veya diğer herkese açık olmayan web siteleri veya Amazon'un veya üçüncü bir tarafın web sitesindeki veya sistemindeki dış ağ hizmetleri (her biri bir "**Dış Ağ**") aracılığı ile, İzin Verilen Amaç için Tedarikçiye Amazon Bilgilerine erişim sağlayabilir. Amazon, Tedarikçinin herhangi bir Amazon Bilgisine bir Dış Ağ kullanarak erişmesine izin verirse Tedarikçi aşağıdaki gerekliliklere uymak zorundadır:

2.2.1 İzin Verilen Amaç. Tedarikçi ve Tedarikçi personeli yalnızca İzin Verilen Amaç için Dış Ağa erişecek ve Amazon Bilgilerine Dış Ağdan erişecek, onları toplayacak, kullanacak, görüntüleyecek, elde edecek, indirecek veya depolayacaktır.

2.2.2 Hesaplar. Tedarikçi, Tedarikçi personelinin yalnızca her birey için Amazon'un belirlediği Dış Ağ hesap(lar)ını kullanmasını sağlayacak ve Tedarikçi personelinin erişim kimlik bilgilerini gizli tutmasını gerekli tutacaktır.

2.2.3 Sistemler. Tedarikçi Dış Ağa yalnızca Tedarikçi tarafından yönetilen işletim sistemlerini çalıştıran ve şunları içeren bilgisayar veya işleme sistemleri veya uygulamaları aracılığı ile erişecektir: (a) Bölüm 2.1.1 (Ağ Güvenliği) uyarınca sistem ağ güvenlik duvarları; (b) Bölüm 2.1.2 (Güncellemeler) uyarınca merkezi yama yönetimi; (c) Bölüm 2.1.3 (Kötü amaçlı yazılımdan koruma) uyarınca işletim sistemine uygun kötü amaçlı yazılımdan koruma yazılımı ve (d) taşınabilir cihazlar için tüm disk şifreleme.

2.2.4 Kısıtlamalar. Amazon tarafından önceden yazılı olarak onaylanması dışında, Tedarikçi herhangi bir Dış Ağdan herhangi bir makine, cihaz veya sunucu dâhil olmak üzere herhangi bir ortama herhangi bir Amazon Bilgisini indirmeyecek, yansıtmayacak veya kalıcı olarak depolamayacaktır.

2.2.5 Hesap Sonlandırma. Tedarikçi, herhangi bir Dış Ağa erişim yetkisi olan: (a) artık Amazon Bilgilerine erişmeye gerek duymayan veya (b) artık Tedarikçi personeli niteliğine sahip olmayan (örneğin, birey Tedarikçinin istihdamından çıkmıştır) herhangi bir Tedarikçi personelinin hesabını sonlandıracak ve en geç 24 saat içinde Amazon'u bilgilendirecektir.

2.2.6 Üçüncü Taraf Sistemleri.

2.2.6.1 Tedarikçi, Amazon Bilgilerini depolayan veya onlara başka bir şekilde erişebilecek olan herhangi bir üçüncü taraf sistemini kullanmadan önce, (a) veriler bu Güvenlik Politikasına göre şifrelenmiş olmadığı ve (b) üçüncü taraf sistemi verilerin şifre çözme anahtarına veya şifrelenmemiş "düz metin" sürümlerine erişmeyecek olmadığı sürece, Amazon'a önceden bildirimde bulunacak ve Amazon'un önceden yazılı onayını alacaktır. Amazon, onay vermeden önce üçüncü taraf sistemi hakkında bir Amazon güvenlik incelemesi yapılmasını (Bölüm 2.5 (Güvenlik İncelemesi) uyarınca) isteme hakkını saklı tutar.

2.2.6.2 Tedarikçinin şifrelenmemiş Amazon Bilgilerini depolayan veya şifrelenmemiş Amazon Bilgilerine başka bir şekilde erişebilen herhangi bir üçüncü taraf sistemini kullanması halinde Tedarikçi üçüncü taraf sistemleri ve bunların güvenlik kontrolleri için bir güvenlik incelemesi gerçekleştirecek ve Amazon'a üçüncü taraf sisteminin güvenlik kontrolleri hakkında Amazon tarafından talep edilen biçim içinde periyodik raporlama sağlayacaktır (örneğin, SAS 70 veya onun ardılı olan rapor veya Amazon tarafından onaylanan daha başka tanınmış endüstri standardı raporlar).

2.3 Veri Saklama ve İmha Etme.

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

2.3.2 İade Etme veya 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 tamamlanmasından veya bu Güvenlik Politikasının feshinden veya sona ermesinden sonra, daha erken olana göre, 30 gün içinde kalıcı ve güvenli şekilde silecektir. Amazon tarafından talep edilmesi halinde Tedarikçi tüm Amazon Bilgilerinin imha edilmiş olduğunu yazılı olarak tasdik edecektir. Açıklık getirmek için, bu bölüm, Bölüm 2.3.3 uyarınca Arşiv Kopyaları için geçerli olmayacaktır

2.3.3 Arşiv Kopyaları. Tedarikçinin yasalar uyarınca vergi veya benzer düzenleyici amaçlar için Amazon Bilgilerinin arşiv kopyalarını saklaması gerekiyorsa bu arşivlenmiş Amazon Bilgileri aşağıdaki yöntemlerden birinde saklanmak zorundadır:

2.3.3.1 Fiziksel olarak güvenli bir tesiste depolanan "soğuk" veya çevrim dışı (yani, anında veya etkileşimli kullanım için hazır olmayan) yedek halinde veya

2.3.3.2 Şifreli dosya(lar)ı barındıran veya depolayan sistemin şifreleme için kullanılan anahtar(lar)ın kopyasına erişiminin olmadığı şifreli şekilde.

2.3.4 Kurtarma. Tedarikçi afetten kurtarma amacı ile bir "kurtarma" (yani bir yedeğe geri dönülmesi) gerçekleştirdiği takdirde Tedarikçi bu Sözleşme veya bu Güvenlik Politikası veya Amazon ile yapılan diğer herhangi bir sözleşme uyarınca silinmesi gereken tüm Amazon Bilgilerinin kurtarma gerçekleştikten sonraki 24 saat içinde bu Bölüm 2.3 uyarınca kurtarılan verilerden yeniden silinmesini veya üzerine yazılmasını sağlayan bir sürece sahip olacak ve bunu sürdürecektir. Tedarikçi herhangi bir amaçla bir kurtarma gerçekleştirirse Amazon'un önceden yazılı onayı olmadan hiçbir Amazon Bilgisi herhangi bir üçüncü taraf sistemine veya ağına kurtarılamaz. Amazon herhangi bir Amazon Bilgisinin herhangi bir üçüncü taraf sistemine veya ağına kurtarılmasına izin vermeden önce üçüncü taraf sistemi veya ağı hakkında bir Amazon güvenlik incelemesi yapılmasını (Bölüm 2.5 (Güvenlik İncelemesi) uyarınca) isteme hakkını saklı tutar.

2.3.5 Veri Temizleme Standartları. Tedarikçi tarafından silinen tüm Amazon Bilgileri, ilgili cihaz türünün temizlenmesi hakkındaki NIST SP 800-88 Revizyon 1, Ortam Temizleme Yönergeleri, 18 Aralık 2014 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf adresinde mevcuttur) Ek A'da yer alan Minimum Temizleme Önerileri uyarınca silinecektir. NIST SP 800-88 Ek A'da ilgili rehberliğin bulunmaması durumunda, Amazon Bilgilerini içeren cihaz şu yollardan biri ile imha edilecektir: (a) manyetik ortamın 10.000+ Gauss elektromanyetik akı alanında manyetikliği giderilerek, (b) 2x2 mm'den küçük parçacıklar ile sonuçlanan şekilde ufalayarak veya mekanik olarak parçalayarak ve (c) Amazon Bilgilerinin sınıflandırılması ve duyarlılığı temelinde Amazon'un isteyebileceği başka standartlar yolu ile.

2.4 Adli İmha. Tedarikçi, Amazon Bilgileri içeren veya herhangi bir zamanda içermiş olan herhangi bir donanımı, yazılımı veya başka bir ortamı elden çıkarmadan (herhangi bir şekilde) önce donanım, yazılım veya başka ortam için Amazon Bilgilerinin herhangi bir şekilde geri alınması olanaksız olacak şekilde tam bir adli imha gerçekleştirecektir. Tedarikçi, adli imhayı, ilgili cihaz türünü imha etmek için NIST SP 800-88 Ek A'da yer alan Minimum Temizleme Önerilerine uygun olarak gerçekleştirecektir.

2.4.1 Tedarikçi, Amazon Bilgileri içeren ve bu Bölüm 2.4'te gerekli tutulan şekilde Tedarikçi tarafından adli olarak imha edilmemiş olan hiçbir donanımı, yazılımı veya başka bir ortamı satmayacak, yeniden satmayacak, bağışlamayacak, yenileştirmeyecek veya başka bir şekilde aktarmayacaktır (bu gibi herhangi bir donanımın, yazılımın veya başka bir ortamın satılması veya aktarılması, Tedarikçinin işinin herhangi bir tasfiyesi ile ilişkili şekilde elden çıkarılması veya başka herhangi bir başka şekilde elden çıkarılması dâhil).

2.5 Güvenlik İncelemesi.

2.5.1 Amazon, Tedarikçinin periyodik olarak Amazon risk değerlendirmesine katılmasını isteme hakkını saklı tutar.

2.5.2 Tasdik. Amazon'un yazılı talebi üzerine, Tedarikçi, risk değerlendirmesinin bir parçası olarak sağlanan bilgilerin Tedarikçi ve Amazon tarafından en son kararlaştırılmış Güvenlik Politikasına uygun olduğunu yazılı olarak Amazon'a tasdik edecektir. Bölüm 1.1 uyarınca Güvenlik Politikasında değişiklikler olması durumunda, bu değişiklikler Tedarikçi ile Amazon arasında anlaşmaya varılıncaya kadar (e-posta yeterli olacaktır) bu Bölümün amaçları için yürürlüğe girmeyecektir.

2.5.3 Diğer İncelemeler. Amazon, Amazon Bilgi Sistemlerinin güvenliğini periyodik olarak inceleme hakkını saklı tutar ancak (a) takvim yılı içinde daha önce önemli bir eksiklik belirlenmediği veya (b) Amazon bir devlet kurumu veya başka bir düzenleyici kurum tarafından söz konusu incelemeyi yapmak zorunda tutulmadığı sürece, yılda bir kereden fazla olmamak üzere. Tedarikçi işbirliği yapacak ve gerekli olan tüm bilgileri makul bir zaman çerçevesi içinde ama Amazon'un talep tarihinden itibaren en çok 20 takvim günü içinde Amazon'a sağlayacaktır.

2.5.4 Düzeltme. Herhangi bir güvenlik incelemesi herhangi bir eksiklik belirlediği takdirde Tedarikçi masrafı ve gideri yalnız Tedarikçiye ait olmak üzere bu eksiklikleri kararlaştırılan bir zaman dilimi içinde düzeltmek için gerekli tüm makul önlemleri alacaktır.

2.6 Güvenlik Vakaları.

2.6.1 Tedarikçi, Amazon Bilgilerine fiili veya kuşku duyulan şekilde yetkisiz olarak erişilmesi, bunların toplanması, elde edilmesi, kullanılması, iletilmesi, açıklanması, kötüye kullanılması veya kaybolması veya herhangi bir Amazon Bilgi Sisteminin ihlal edilmesi (bir "**Güvenlik Vakası") hakkında Tedarikçinin bilgi sahibi olmasından sonra olanaklı olan en kısa sürede ama en geç 24 saat içinde Amazon'u bilgilendirecektir**. Tedarikçi her Güvenlik Vakasını zamanlı şekilde düzeltecek ve Tedarikçinin her Güvenlik Vakası ile ilgili iç soruşturması hakkında Amazon'a yazılı ayrıntılar sağlayacaktır. Geçerli yasalar izin verdiği zaman, Amazon Tedarikçiden yazılı olarak özellikle talep etmediği sürece Tedarikçi Amazon adına hiçbir düzenleyici makama veya müşteriye bildirimde bulunmamayı kabul etmektedir ve herhangi bir tarafa herhangi bir bildirim sunulmadan önce Amazon onun biçimini ve içeriğini inceleme ve onaylama hakkını saklı tutar. Tedarikçi, teyit edilmiş tüm Güvenlik Vakalarını düzeltmek için bir plan formüle etmek ve uygulamak üzere Amazon ile işbirliği yapacak ve birlikte çalışacaktır.

2.6.2 Geçerli yasanın izin verdiği ölçüde, Tedarikçinin bir devlet kurumundan herhangi bir Amazon Bilgisi içeren veriler isteyen bir talep veya emir (bir mahkeme celbi, mahkeme emri veya arama emri gibi) alması durumunda, Tedarikçi Amazon'a Amazon'un koruyucu bir emir veya başka uygun bir çözüm aramasını sağlamaya yetecek şekilde bildirimde bulunacaktır.

2.7 Genel. Amazon, bu Güvenlik Politikası kapsamında tüm geçerli kararları alma konusunda tek takdir yetkisine sahiptir. "Dâhil" veya "örneğin" ibarelerini izleyen herhangi bir örnek listesi açıklayıcıdır ve tam kapsamlı değildir. Bu Güvenlik Politikası kapsamında güvenlik gereklilikleri için standartlara yapılan tüm atıflar, Amazon aksini belirtmediği sürece, güncellenmiş olabilecek şekli ile belirtilen standartları ve bunların ilgili ardıl sürümlerini veya eşdeğer sürümlerini belirtir.