

**Tedarikçi ve
Hizmet Sağlayıcı
Bilgi Güvenliği Yönetimi
Politikası**

▶ 1-2

Redstar Havacılık (RSA), faaliyetlerinin yürütülmesinde yararlanılan tedarikçi, hizmet sağlayıcı, iş ortağı ve diğer üçüncü taraflarla ilişkilerin; bilgi güvenliği, operasyonel süreklilik, havacılık emniyeti ve uygulanabilir yasal, düzenleyici ve sözleşmesel gereklilikler dikkate alınarak yönetilmesini taahhüt etmektedir.

Bu politikanın amacı; RSA bilgi varlıklarına, sistemlerine, verilerine veya tesislerine erişen ya da RSA adına hizmet sunan üçüncü taraflardan kaynaklanabilecek bilgi güvenliği risklerinin uygun şekilde yönetilmesini ve tedarikçi ilişkilerinin yaşam döngüsü boyunca gerekli güvenlik şartlarının uygulanmasını sağlamaktır.

RSA, tedarikçi ve hizmet sağlayıcı ilişkilerinde bilgi güvenliğinin yalnızca sözleşme aşamasında değil; seçim, değerlendirme, hizmet sunumu, değişiklik ve hizmetin sonlandırılması dahil olmak üzere ilişkinin tüm yaşam döngüsü boyunca yönetilmesi gerektiğini kabul etmektedir.

Bu kapsamda RSA;

- Tedarikçi ve hizmet sağlayıcıları; sundukları hizmetin kritikliği, eriştikleri bilgi ve sistemler, işlenen verilerin hassasiyeti ve faaliyetler üzerindeki potansiyel etkileri doğrultusunda risk temelli bir yaklaşımla değerlendirir ve sınıflandırır.
- Kritik ve bilgi güvenliği açısından önemli tedarikçiler için, belirlenen risk seviyesine uygun güvenlik gereksinimlerinin oluşturulmasını ve uygulanmasını sağlar.
- Tedarikçi seçim ve ön değerlendirme süreçlerinde; hizmet kapsamı, bilgi güvenliği kabiliyetleri, iş sürekliliği, veri işleme koşulları, alttedarikçi kullanımı ve ilgili diğer güvenlik unsurlarının değerlendirilmesini destekler.
- Tedarikçi ilişkilerinden kaynaklanan bilgi güvenliği risklerinin BGYS risk yönetimi süreçleri kapsamında belirlenmesini, değerlendirilmesini, izlenmesini ve gerekli durumlarda uygun risk işleme faaliyetlerinin uygulanmasını sağlar.
- Tedarikçi ve hizmet sağlayıcılarla yapılan sözleşmelerde; hizmetin niteliği ve risk seviyesi doğrultusunda gizlilik, bilgi sınıflandırma, erişim kontrolü, olay ve ihlal bildirimi, hizmet seviyeleri, iş sürekliliği, yedekleme, veri güvenliği, şifreleme, alt tedarikçi kullanımı, denetim hakkı ve hizmet sonlandırma şartlarının uygun şekilde ele alınmasını sağlar.
- RSA bilgi varlıklarına ve sistemlerine sağlanan üçüncü taraf erişimlerinin iş ihtiyacı ile sınırlı, yetkilendirilmiş, kontrollü ve gerektiğinde izlenebilir olmasını esas alır.
- Tedarikçi performansının, hizmet seviyesi taahhütlerinin ve uygulanabilir bilgi güvenliği gereksinimlerine uyumun risk seviyesine uygun olarak izlenmesini ve değerlendirilmesini destekler.
- Tedarikçi veya hizmet sağlayıcılardan kaynaklanan bilgi güvenliği olaylarının ve ihlal şüphelerinin RSA bilgi güvenliği olay yönetimi süreçleri doğrultusunda raporlanmasını, değerlendirilmesini ve yönetilmesini sağlar.
- Tedarikçi hizmetlerinde gerçekleştirilen ve RSA'nın bilgi güvenliği, operasyonel süreklilik veya kritik süreçleri üzerinde etkisi olabilecek değişikliklerin değerlendirilmesini ve gerekli durumlarda risk ve değişiklik yönetimi süreçlerine dahil edilmesini sağlar.



- Bulut hizmetleri ve üçüncü taraf bilgi sistemlerinin kullanımında; veri lokasyonu, veri aktarımı, erişim güvenliği, hizmet sürekliliği, alt hizmet sağlayıcı kullanımı ve diğer uygulanabilir bilgi güvenliği gereksinimlerinin değerlendirilmesini esas alır.
- Tedarikçinin alt tedarikçi kullanması durumunda, RSA bilgi varlıkları ve hizmetleri üzerinde etkisi olabilecek alt tedarikçi ilişkilerinden kaynaklanan risklerin değerlendirilmesini ve gerekli güvenlik şartlarının ilgili taraflara yansıtılmasını destekler.
- Hizmet ilişkisinin sona ermesi veya tedarikçi değişikliği durumunda; RSA'ya ait bilgi ve varlıkların geri alınması, üçüncü taraf erişimlerinin sonlandırılması, gerekli veri silme veya imha işlemlerinin gerçekleştirilmesi ve kritik hizmetlerde operasyonel sürekliliğin korunmasını esas alır.
- Kritik hizmetlerde tedarikçi bağımlılığından kaynaklanabilecek süreklilik risklerini değerlendirir ve gerektiğinde alternatif hizmet, geçiş veya iş sürekliliği düzenlemelerinin oluşturulmasını destekler.
- Tedarikçi ve hizmet sağlayıcılarla ilişkilerde uygulanabilir yasal, düzenleyici, sözleşmesel, kişisel veri koruma ve müşteri gerekliliklerinin karşılanmasını gözetir.
- Tedarikçi yönetimi kapsamında tespit edilen uygunsuzlukların, güvenlik zafiyetlerinin veya kontrol eksikliklerinin ilgili düzeltici ve iyileştirici faaliyet süreçleri kapsamında ele alınmasını sağlar.
- Politika gerekliliklerinden sapılması gereken durumlarda, istisnaların risk temelli olarak değerlendirilmesini, yetkili kişiler tarafından onaylanmasını, gerekli telafi edici kontrollerin belirlenmesini ve kayıt altına alınmasını sağlar.

RSA, tedarikçi ve hizmet sağlayıcı ilişkilerinin güvenli ve etkin şekilde yönetilmesinin; bilgi güvenliğinin, operasyonel dayanıklılığın, iş sürekliliğinin ve havacılık emniyetinin korunmasının önemli bir unsuru olduğunu kabul etmektedir.

Bu Politika; RSA'ya hizmet sağlayan, RSA bilgi varlıklarına, bilgi sistemlerine, verilerine veya tesislerine erişen ya da RSA adına bilgi işleyen tüm tedarikçileri, hizmet sağlayıcıları, danışmanları, dış kaynak personeli, iş ortaklarını, alt tedarikçileri ve ilgili diğer üçüncü tarafları kapsar.

Politika; ISO/IEC 27001:2022 kapsamında tedarikçi ilişkileri, tedarikçi anlaşmaları, tedarikçi hizmetlerinin izlenmesi ve değişiklik yönetimi ile bulut hizmetlerinin kullanımına ilişkin bilgi güvenliği gereklilikleri dikkate alınarak uygulanır.

Tedarikçi ve Hizmet Sağlayıcı Yönetimi Politikası;

- Dokümanite edilmiş bilgi olarak oluşturulur, sürdürülür ve kontrol edilir.
- Kuruluş içerisinde ilgili çalışanlara duyurulur ve erişilebilir durumda tutulur.
- Uygun olduğu ölçüde tedarikçilere, hizmet sağlayıcılara ve diğer ilgili taraflara sunulur.
- En az yılda bir kez ve ayrıca tedarikçi yapısında, hizmet modellerinde, teknolojik altyapıda, yasal veya düzenleyici gerekliliklerde ya da bilgi güvenliği risklerinde önemli değişiklikler olması durumunda gözden geçirilir ve gerekli görüldüğünde güncellenir.

Sorumlu Müdür/CEO

