- **1. Amaç**

Bu politikanın amacı, Beşiktaş Tersane A.Ş.'nin tedarikçileri, alt yükleniciler, danışmanlar ve diğer dış hizmet sağlayıcılarıyla kurduğu ilişkilerde bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunmasını güvence altına almaktır. Şirketimiz, tedarik zincirinde oluşabilecek bilgi güvenliği risklerini en aza indirmeyi ve ilgili tüm taraflarla şeffaf, denetlenebilir ve standartlara uygun bir ilişki yönetimi sağlamayı taahhüt eder.

- **2. Kapsam**

Bu politika; Beşiktaş Tersane A.Ş. adına mal veya hizmet temin eden, şirketin bilgi sistemlerine, tesislerine veya verilerine erişimi olan tüm tedarikçileri, taşeronları, danışmanlık firmalarını, bulut/BT hizmet sağlayıcılarını ve lojistik/iş ortaklarını kapsar. Politika, tedarikçi seçiminden sözleşme sonlandırmasına kadar olan tüm yaşam döngüsünü içerir.

- **3. Politika İlkeleri**
- **3.1. Tedarikçi Seçimi ve Risk Değerlendirmesi**
- Yeni bir tedarikçiyle çalışmaya başlamadan önce, tedarikçinin bilgi güvenliği açısından oluşturabileceği risk seviyesi belirlenir.
- Kritik veya hassas veriye erişimi olacak tedarikçiler için bilgi güvenliği yeterlilik değerlendirmesi yapılır.
- Gerekli görülen durumlarda tedarikçiden ISO 27001 sertifikası, bağımsız denetim raporu veya eşdeğer güvence belgeleri talep edilir.
- **3.2. Sözleşmesel Güvenlik Gereksinimleri**
- Tüm tedarikçi sözleşmelerine bilgi güvenliği şartları (gizlilik, veri koruma, erişim kontrolü, bildirim yükümlülükleri) madde olarak eklenir.
- Kişisel veri işleyen tedarikçilerle KVKK ve ilgili mevzuata uygun veri işleme sözleşmeleri (VİS) imzalanır.
- Sözleşmelerde, tedarikçinin alt yüklenici kullanması durumunda aynı güvenlik yükümlülüklerinin devredilmesi şartı yer alır.
- Fikri mülkiyet, bilgi varlıklarının iadesi/imhası ve sözleşme sonu yükümlülükleri açıkça tanımlanır.

- **3.3. Erişim Yönetimi**
- Tedarikçilere şirket sistemlerine veya tesislerine erişim, yalnızca iş gereksinimi doğrultusunda ve “bilmesi gereken” (need-to-know) ilkesiyle tanımlanır.
- Tüm tedarikçi erişimleri kayıt altına alınır, düzenli olarak gözden geçirilir ve iş ilişkisi sona erdiğinde derhal kapatılır.
- Uzaktan erişim gerektiren durumlarda güvenli bağlantı yöntemleri (VPN, çok faktörlü kimlik doğrulama vb.) zorunludur.
- **3.4. İzleme, Denetim ve Performans Değerlendirmesi**
- Kritik tedarikçilerin bilgi güvenliği performansı periyodik olarak izlenir ve değerlendirilir.
- Gerekli görüldüğünde tedarikçi tesislerinde veya sistemlerinde bilgi güvenliği denetimi yapma hakkı saklıdır.
- Tedarikçi kaynaklı bilgi güvenliği olayları, şirketin olay yönetimi prosedürleri kapsamında ele alınır ve kök neden analizi yapılır.
- **3.5. Bilgi Güvenliği Olayı Bildirimi**
- Tedarikçiler, bilgi güvenliğini etkileyebilecek herhangi bir olay, ihlal veya şüpheli durumu derhal Beşiktaş Tersane A.Ş.’ye bildirmekle yükümlüdür.
- Bildirim süreleri ve usulleri ilgili sözleşmelerde ayrıca tanımlanır.
- **3.6. Sözleşme Sonlandırma ve Çıkış Süreci**
- İş ilişkisinin sona ermesi durumunda tüm erişim hakları iptal edilir, fiziksel ve dijital varlıklar iade alınır veya güvenli şekilde imha edilir.
- Tedarikçinin işlediği veriler, sözleşme ve yasal gereklilikler doğrultusunda silinir veya iade edilir; bu işlem belgelenir.

GENEL MÜDÜR

Ş.MURAT BENER