



T.C. SAĞLIK BAKANLIĞI

MAL VE HİZMET ALIM GÜVENLİĞİ PROSEDÜRÜ

S.B.Ü
GAZİ YAŞARGİL EĞİTİM
VE
ARAŞTIRMA HASTANESİ

Kodu	Yayınlanma Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
				1 / 2

1. AMAÇ

Bu doküman, S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi bünyesinde yapılan mal ve hizmet alımlarında uyulması gereken T.C. Sağlık Bakanlığı Diyarbakır İl Sağlık Müdürlüğü Bilgi Güvenliği politikasını tanımlamaktadır.

2. KAPSAM

Bu prosedür S.B.Ü. Diyarbakır Gazi Yaşargil Eğitim ve Araştırma Hastanesi bünyesinde yapılan mal ve hizmet alımları ile alım sürecinde görevyapan tüm kişileri kapsamaktadır.

3. UYGULAMA

- 3.1.** Mal ve hizmet alımlarında ilgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilmelidir.
- 3.2.** Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır:
 - 3.2.1.** Bilgi güvenliği politikası,
 - 3.2.2.** Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,
 - 3.2.3.** Gerekli fiziki koruma için kontrol ve mekanizmalar, Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,
 - 3.2.4.** Anlaşma sırasında, sonrasında ya da zaman içinde kabul edilen bir noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,
 - 3.2.5.** Varlıklarla ilgili gizlilik, bütünlük, erişilebilirlik özellikleri,
 - 3.2.6.** Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,
 - 3.2.7.** Kullanıcı ve yönetici eğitimlerinin methodu, prosedürü ve güvenliği,
 - 3.2.8.** Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar,
 - 3.2.9.** Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları,
 - 3.2.10.** İzin verilen erişim yöntemleri, kullanıcı kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,
 - 3.2.11.** Anlaşmayla ilgili tarafların yükümlülükleri,
 - 3.2.12.** Hukuki konularla ilgili sorumlulukları ve yasal gereklerin nasıl karşılanması gerektiğinden emin olunmalıdır, (örneğin, veri koruma mevzuatı, anlaşma diğer ülkelerle ile işbirliği içeriyorsa özellikle farklı ulusal yargı sistemleri dikkate alınarak)
 - 3.2.13.** Fikri mülkiyet hakları (IPRs), telif hakkı ve herhangi bir ortak çalışmanın korunması,
 - 3.2.14.** Anlaşmaların yeniden müzakeresi ya da feshi için şartlar,
- 3.3.** Farklı kuruluşlar ve farklı türdeki üçüncü taraflar arasında yapılan anlaşmalar önemli ölçüde değişebilir. Bu nedenle; anlaşmalar, belirlenen tüm riskleri ve güvenlik gereklerini içerecek şekilde yapılmalıdır. Gerektiğinde güvenlik yönetim planındaki gerekli kontroller ve prosedürler genişletilebilir.
- 3.4.** Üçüncü taraflarla yapılan anlaşmalar diğer tarafları içerebilir. Üçüncü taraflara erişim hakkı

Hazırlayan	Kontrol Eden	Onaylayan



T.C. SAĞLIK BAKANLIĞI

MAL VE HİZMET ALIM GÜVENLİĞİ PROSEDÜRÜ

S.B.Ü
GAZİ YAŞARGİL EĞİTİM
VE
ARAŞTIRMA HASTANESİ

Kodu	Yayınlanma Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
				2 / 2

verilmeden önce, erişim hakkı ve katılım için diğer tarafların ve koşulların belirlenmesi amacıyla anlaşmaya varılması gerekir.

3.5. Gizlilik Sözleşmeleri

- 3.5.1. Gizlilik veya ifşa etmeme anlaşmaları yasal olarak uygulanabilir terimleri kullanarak gizli bilgileri korumanın gerekliliğini ele almalıdır.
- 3.5.2. Gizlilik veya ifşa etmeme anlaşmaları için aşağıdaki unsurlar dikkate alınmalıdır:
 - 3.5.2.1. Korunacak bilginin bir tanımı (örneğin; gizli bilgileri),
 - 3.5.2.2. Gizliliğin süresiz muhafaza edilmesi gereken durumlar da dâhil olmak üzere anlaşma süresi,
 - 3.5.2.3. Anlaşma sona erdiğinde yapılması gereken eylemler,
 - 3.5.2.4. Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar ve imza eylemlerinin belirlenmesi ('bilmesi gereken' gibi),
 - 3.5.2.5. Bilginin sahibinin, ticari sırların ve fikri mülkiyet haklarının ve bu gizli bilgilerin nasıl korunması gerektiği,
 - 3.5.2.6. Gizli bilgilerin kullanım izni ve bilgileri kullanmak için imza hakları,
 - 3.5.2.7. Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı, Yetkisiz açıklama ya da gizli bilgilerin ihlal edilmesinin bildiri ve raporlama süreci,
 - 3.5.2.8. İade veya imha anlaşmasına bırakılacak bilgi için terimler,
 - 3.5.2.9. Bu anlaşmanın ihlali durumunda yapılması beklenen eylemler.
- 3.5.3. Bir kuruluşun güvenlik gereksinimlerine dayalı olarak, diğer unsurlarla bir gizlilik veya ifşa etmeme anlaşması gereklidir.
- 3.5.4. Gizlilik ve ifşa etmeme anlaşmaları uygulandığı yerin geçerli tüm yasa ve yönetmeliklerine uygun olmalıdır.
- 3.5.5. Gizlilik ve ifşa etmeme anlaşmaları için gerekler periyodik olarak veya gerekleri etkileyecek bir değişiklik olduğunda gözden geçirilmelidir.
- 3.5.6. Gizlilik ve ifşa etmeme anlaşmaları kurumsal bilgileri korumalı ve imzalayanın, bilginin korunmasından, kullanılmasından ve ifşa edilmesinden yetkili ve sorumlu olduğunu belirtmelidir.
- 3.5.7. Farklı koşullarda gizlilik ve ifşa etmeme anlaşmaları kuruluşun ihtiyaçları doğrultusunda farklı şekillerde kullanılmalıdır.
- 3.5.8. Üçüncü taraflardan yapılacak mal ve hizmet alımlarında **Kurumsal Gizlilik Taahhünamesi** imzalanmalıdır.

4. YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla **BGYS Disiplin Prosedürü** Dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

Hazırlayan	Kontrol Eden	Onaylayan