|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **MAL VE HİZMET ALIM GÜVENLİĞİ** | | | C:\Users\olympos\Desktop\antalya_ism_logo 800x600.jpg |
| **Kodu** | **Yayınlama tarihi** | **Revizyon Tarihi** | **Revizyon No** | **Sayfa** |
| **BG.PR.06** | **20.10.2015** | **20.10.2015** |  | **1/3** |

1. Mal ve hizmet alımlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnamelerde belirtilmelidir.
2. Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır:

• Bilgi güvenliği politikası,

• Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,

• Gerekli fiziki koruma için kontrol ve mekanizmalar,

• Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,

• Varlıklarda oluşan herhangi bir değişimin tespiti için prosedürler; örneğin, bilgi, yazılım ve donanımda oluşan kayıp veya modifikasyon,

• Anlaşma sırasında, sonrasında ya da zaman içinde kabul edilen bir noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,

• Varlıklarla ilgili gizlilik, bütünlük, elverişlilik ve başka özellikleri,

• Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,

• Kullanıcı ve yönetici eğitimlerinin methodu, prosedürü ve güvenliği,

• Bilgi güvenliği sorumluluğu ve sorunları için kullanıcı bilinci sağlama,

• Uygun olduğu yerde personel transferi için hüküm,

• Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar,

• Açık bir raporlama yapısı ve anlaşılan raporlama formatı,

• Değişim yönetimi sürecinin açıkça belirlenmesi,

• Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları,

• İzin verilen erişim yöntemleri, kullanıcı kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,

• Kullanıcı erişimi ve ayrıcalıkları için bir yetkilendirme süreci,

• Korumanın bir gerekliliği olarak mevcut hizmetleri kullanmaya yetkili kişilerin ve hakları ile ayrıcalıkları gibi kullanımları ile ilgili olan bir bilgilerin bir listesi,

• Erişim haklarının iptal edilmesi veya sistemler arası bağlantı kesilmesi için süreç,

• Sözleşme de belirtilen şartların ihlali olarak meydana gelen bilgi güvenliği ihlal olaylarının ve güvenlik ihlallerinin raporlanması, bildirimi ve incelenmesi için bir anlaşma,

• Sağlanacak ürün veya hizmetin bir açıklaması ve güvenlik sınıflandırması ile kullanılabilir hale getirilmesini tanımlayan bir bilgi,

• Hedef hizmet seviyesi ve kabul edilemez hizmet seviyesi,

• Doğrulanabilir performans kriterlerinin tanımı, kriterlerin izlenmesi ve raporlanması,

• Kuruluşun varlıkları ile ilgili herhangi bir faaliyetin izlenmesi ve geri alınması hakkı,

• Üçüncü bir taraf tarafından yürütülen denetimler için sözleşmede belirtilen denetleme sorumlulukları hakkı ve denetçilerin yasal haklarının sıralanması,

• Sorun çözümü için bir yükseltme sürecinin kurulması,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **MAL VE HİZMET ALIM GÜVENLİĞİ** | | | C:\Users\olympos\Desktop\antalya_ism_logo 800x600.jpg |
| **Kodu** | **Yayınlama tarihi** | **Revizyon Tarihi** | **Revizyon No** | **Sayfa** |
| **BG.PR.06** | **20.10.2015** | **20.10.2015** |  | **2/3** |

• Bir kuruluşun iş öncelikleri ile uygun elverişlilik ve güvenilirlik de dahil olmak üzere hizmet sürekliliği gerekleri,

• Anlaşmayla ilgili tarafların yükümlülükleri,

• 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)

• Fikri mülkiyet hakları (IPRs), telif hakkı ve herhangi bir ortak çalışmanın korunması,

• Üçüncü tarafların alt yüklenicileri ile birlikte bağlılığı ve altyüklenicilere uygulanması gereken güvenlik kontrolleri,

• Anlaşmaların yeniden müzakeresi ya da feshi için şartlar,

• Taraflardan birinin anlaşmayı planlanan tarihten önce bitirmesi durumunda bir acil durum planı olmalıdır.

• Kuruluş güvenlik gereklerinin değişmesi durumunda anlaşmaların yeniden müzakere edilmesi,

• Varlık listeleri, lisanslar, anlaşmalar ve hakların geçerli belgeleri ve onlarla ilişkisi.

1. 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.
2. Bilgi güvenliği yönetimi dış kaynaklı ise anlaşmalarda üçüncü tarafın güvenlik garantisinin yeterliliğini nasıl ele alındığı anlaşmada belirtilmelidir. Risk değerlendirmede tanımlandığı gibi, risklerdeki değişiklikleri belirlemek ve başa çıkmak için güvenliğin nasıl adapte edileceği ve sürdürüleceği ele alınmalıdır.
3. Dış kaynak kullanımı ve üçüncü taraf hizmet sunumunun diğer formları arasındaki farklılıkların bazıları; sorumluluk, geçiş durumu planlama ve işlemler süresince potansiyel kesinti süresi, acil durum planlaması yönetmelikleri ve durum tespitinin gözden geçirilmesi, güvenlik olayları hakkında bilgi toplanması ve yönetimi konularında sorular içerecektir. Bu nedenle, dış kaynaklı bir yönetmelik geçişinde; kuruluş değişiklikleri yönetmek için uygun süreçlere ve anlaşmaların yeniden müzakere edilmesi ya da fesh edilmesi hakkına sahip olduğu için kuruluşun planlaması ve yönetimi önemlidir.
4. Üçüncü taraflarla yapılan anlaşmalar diğer tarafları içerebilir. Üçüncü taraflara erişim hakkı verilmeden önce, erişim hakkı ve katılım için diğer tarafların ve koşulların belirlenmesi amacıyla anaşmaya varılması gerekir.
5. Genellikle anlaşmaların esasları kuruluşlar tarafından geliştirilmiştir. Bazı durumlarda anlaşmaların üçüncü taraflarca geliştirilmesi ve kuruluşa empoze edilmesi durumu olabilir. Kuruluşlar, kendi yapılarına üçüncü taraflarca empoze edilecek anlaşmalarda kendi güvenliklerinin gereksiz yere etkilenmesini engeller.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **MAL VE HİZMET ALIM GÜVENLİĞİ** | | | C:\Users\olympos\Desktop\antalya_ism_logo 800x600.jpg |
| **Kodu** | **Yayınlama tarihi** | **Revizyon Tarihi** | **Revizyon No** | **Sayfa** |
| **BG.PR.06** | **20.10.2015** | **20.10.2015** |  | **3/3** |

1. **Gizlilik Sözleşmeleri**
2. Gizlilik veya ifşa etmeme anlaşmaları yasal olarak uygulanabilir terimleri kullanarak gizli bilgileri korumanın gerekliliğini ele almalıdır. Gizlilik veya ifşa etmeme anlaşmaları için aşağıdaki unsurlar dikkate alınmalıdır:

• Korunacak bilginin bir tanımı (örneğin; gizli bilgileri),

• Gizliliğin süresiz muhafaza edilmesi gereken durumlar da dahil olmak üzere anlaşma süresi,

• Anlaşma sona erdiğinde yapılması gereken eylemler,

• Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar ve imza eylemlerinin belirlenmesi (‘bilmesi gereken’ gibi),

• Bilginin sahibinin, ticari sırların ve fikri mülkiyet haklarının ve bu gizli bilgilerin nasıl korunması gerektiği,

• Gizli bilgilerin kullanım izni ve bilgileri kullanmak için imza hakları,

• Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı,

• Yetkisiz açıklama ya da gizli bilgilerin ihlal edilmesinin bildirimi ve raporlama prosesi,

• İade veya imha anlaşmasına bırakılacak bilgi için terimler,

• Bu anlaşmanın ihlali durumunda yapılması beklenen eylemler.

1. Bir kuruluşun güvenlik gereksinimlerine dayalı olarak, diğer unsurlarla bir gizlilik veya ifşa etmeme anlaşması gereklidir.
2. Gizlilik ve ifşa etmeme anlaşmaları uygulandığı yerin geçerli tüm yasa ve yönetmeliklerine uygun olmalıdır.
3. Gizlilik ve ifşa etmeme anlaşmaları için gerekler periyodik olarak veya gerekleri etkileyecek bir değişiklik olduğunda gözden geçirilmelidir.
4. Gizlilik ve ifşa etmeme anlaşmaları kurumsal bilgileri korumalı ve imzalayanın, bilginin korunmasından, kullanılmasından ve ifşa edilmesinden yetkili ve sorumlu olduğunu belirtmelidir.
5. Farklı koşullarda gizlilik ve ifşa etmeme anlaşmaları kuruluşun ihtiyaçları doğrultusunda farklı şekillerde kullanılmalıdır

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **HAZIRLAYAN**  **(Bilgi Güvenliği Komisyonu)** | | | | | |
| *Komisyon Başkanı*  Bülent YURTERİ  Şube Müdürü | *Başkan Yardımcısı*  Ersin HOŞER  V.H.K.İ | *Üye*  Okşan Duru ÖZDAĞ  Doktor | *Üye*  Demet KILIÇ  Avukat | *Üye*  Osman ÜNAY  Bilgisayar Mühendisi | *Üye*  K. Erkan AKKUŞ  Bilgisayar Mühendisi |
|  |  |  |  |  |  |
| *Üye (Eğitimci)*  Ünal GÖKÇE  Sağlık Memuru | *Bilgi Güvenliği Yetkilisi*  Özgür AYDIN  Programcı | *Üye*  Fethi ÇELİK  Programcı | *Üye*  İsmail ÇİFTÇİ  Bilgisayar İşletmeni | *Üye*  Okkan KARADAŞ  Tıbbi Sektreter |  |

**O N A Y**

…/…/2015

Dr. Ünal HÜLÜR

İl Sağlık Müdürü