1.AMAÇ

Bu prosedür T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı ve T.C. Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi ve Kılavuzu hükümleri gereği ve aşağıdaki kapsam maddesi dahilinde, Hatay İl Sağlık Müdürlüğü hizmet verdiği Sağlık Bilgi sistemleri servis hizmetlerinin kullanılması dahilinde, talep eden Özel Firmalar ve Kamu Kurumları ile Hatay İl Sağlık Müdürlüğünün sunmuş olduğu bilgi işlem hizmetlerini kullanmak üzere başvuruda bulunanlar, yada istihdam ettirilen personel ile yapılması gereken Personel Gizlilik Sözleşmesi ve Kurumsal Gizlilik Sözleşmesinin uygulanmasını amaçlar.

2.KAPSAM

Hatay İl Sağlık Müdürlüğü Sağlık Bilgi Sistemleri Şube Müdürlüğü tarafından sunmuş olduğu bilgi işlem hizmetlerinden yararlanmak isteyen Kurumlar, Yüklenici ve alt yüklenici firmalar ile bu kurumlarda çalışan personelleri ile İl Sağlık Müdürlük bünyesinde çalışmakta olan tüm personeli (4a,4b,4c, Danışman, Firma personeli} kapsamaktadır.

3.UYGULAMA

Hatay İl Sağlık Müdürlüğü Sağlık Bilgi Sistemleri Şube Müdürlüğü tarafından sunmuş olduğu bilgi işlem hizmetlerinden yararlanmak isteyen Kurumlar, Yüklenici ve alt yüklenici firmalar ile bu kurumlarda çalışan personelleri ile İl Sağlık Müdürlük bünyesinde çalışmakta olan tüm personeli (4a,4b,4c, Danışman, Firma personeli) kapsamaktadır.

4.MAL VE HİZMET ALIM GÜVENLİĞİ POLİTİKALARI

4.1. Mal ve hizmet atımlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabet engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilmelidir,

4.2. Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır,

4.3. Bilgi güvenliği politikası,

4.4. Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,

4.5. Gerekli fiziki koruma için kontrol ve mekanizmalar,

4.6.Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,

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

4.8. Anlaşma sırasında, sonrasında ya da zaman içinde kabul edilen hır noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,

4.9. Varlıklarla, ilgili gizlilik, bütünlük, elverişlilik ve başka özellikleri,

4.10. Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,

4.11. Kullanıcı ve yönetici eğitimlerinin metodu prosedürü ve güvenliği,

4.12. Bilgi güvenliği sorumluluğu ve sorunlar için kullanıcı bilinci sağlama,

4.13. Uygun olduğu yerde personel transferi için hüküm,

4.14. Donanım ve yazılın kurulumu ve bakımı ile ilgili sorumlular,

4.15.Açık bir raporlama yapısı ve anlaşılan raporlama formatı,

4.16. Değişim yönelimi sürecinin açıkça belirlenmesi,

4.17. Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları izin verilen erişim yöntemleri, kullanma kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,

4.18. Kullanıcı erişimi ve ayrıcalıkları için bir yetkilendirme süreci,

4.19. Korumanın bir gerekliliği olarak mevcut hizmetten kullanmaya yetkili kişilerin ve hakları ile ayrıcalıkları gibi kullanımları ile ilgili olan bir bilgilerin bir listesi,

4.20. Erişini haklarının iptal edilmesi veya sistemler arası bağlantısı kesilmesi için süreç,

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

4.22. Sağlanacak ürün veya hizmetin bir açıklaması ve güvenlik sınıflandırması He kullanılabilir hale getirilmesini tanımlayan bir bilgi,

4.23. Hedef hizmet seviyesi ve kabul edilemez hizmet seviyesi,

4.24. Doğrulanabilir performans kriterlerinin tanımı, kriterlerin izlenmesi ve raporlanması,

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

4.26.Üçüncü bir tara!' tarafından yürütülen denetimler için sözleşmede belirtilen denetleme sorumlulukları hakkı ve denetçilerin yasal haklarının sıralanması,

4.27. Sorun çözümü için bir yükseltme sürecinin kurulması,

4.28. Bir kuruluşun iş öncelikleri ile uygun elverişlilik ve güvenilirlik, de dâhil olmak tere hizmet sürekliliği gerekler,

4.29. Anlaşmayla ilgili taraftarın yükümlülükleri,

4.30. Hukuki konularla ilgili sorumlulukları ve yasal gereklerin nasıl karşılanması gerektiğinden emin olunmalıdır, (örneğim veri koruma mevzuatı, anlaşma diğer ülkelerle ile işbirliği içeriyorsa özellikle farklı ulusal yargı sistemleri dikkate alınarak),

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

2/3

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

4.33. Anlaşmaların yeniden müzakeresi ya da feshi için şanlar,

4.34. Taraflardan birinin ani aşmayı planlanan tarihten önce bitirmesi durumunda bir acil durum planı olmalıdır,

4.35. Kuruluş güvenlik gereklerinin değişmesi durumunda anlaşmaların vadiden müzakere edilmesi,

4.36. Varlık üsteleri, lisanslar, anlaşmalar ve hakların geçerli belgeleri ve onlarla ilişkisi

4.37. Farklı kuruluşlar ve farklı türdeki üçüncü taraftar arabanda 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,

4.38. 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.

4.39.Dış kaynak kullanımı ve üçüncü taraf hizmet sunumunun diğer formları arasındaki farklılıkların bazıları; sorumluluk, geçiş durumu planlama ve işlemler süresince potansiyel kesimi süresi acil durum planlaması yönetmelikten ve durum tespitinin gözden geçirilmesi, güvenlik olayları hakkında bilgi toplanması ve yönetimi konularında sorular içerecektir. Bu nedenle, dış kaynaklı bir yönetmelik geçişinde, kuruluş değişiklikleri yönelmek için uygun süreçlere ve anlaşmaların yemden müzakere edilmesi ya da test edilmesi hakkına sahip olduğu için kuruluşun planlaması ve yönetimi önemlidir.

4.40.Üçüncü taraflarla yapılan anlaşmalar diğer tarafları içerebilir. Üçüncü taraflara erişim hakkı verilin eden önce, erişim hakkı ve kâtibin için diğer tarafken ve koşullan belirlenmesi amacıyla anlaşmaya varılması gerekir,

4.41. Genellikle anlaşmaların esasları kuruluşlar taralından 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,

4.42.Gizlilik Sözleşmeleri

4.42.1. 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

4.42.2. Korunacak bilginin bir tanımı (örneğin; gizli bilgileri),

4.42. Gizliliğin süresiz muhafaza edilmesi gereken durumlar da dâhil olmak üzere anlaşma süresi,

4.42.3. Anlaşma sona erdiğinde yapılması gereken eylemler,

4.42.4. Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar ve imza eylemlerinin belirlenmesi ('bilmesi gereken' gibi),

4.42.5. Bilginin sahihinin, ticari sırların ve fikri mülkiyet haklanın ve bu gizli bilgilerin nasıl korunması gerektiği,

4.42.6. Gizli bilgilerin kullanım izni ve bilgileri kullanmak için imza hakları.

4.42.7. Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı.Yetkisiz açıklama ya da gizli bilgilenil ihlal edilmesinin bildirimi ve raporlama prosesi,

4.43.İade veya imim anlaşmasına bırakılacak bilgi için terimler,

4.44.Bu anlatmanın ihlali durumunda yapılması beklenen eylemler,

4.44.1. Bir kuruluşun güvenlik gereksinimlerine dayalı olarak, diğer unsurlarla hır gizlilik veya ifşa etmeme anlaşması gereklidir.

4.44.2. Gizlilik ve ifşa etmeme anlaşma6ları uygulandığı yeni geçerli tüm yasa ve yönetmeliklerine uygun olmalıdır.

4.44.3. Gizlilik ve ifşa etmeme anlaşmaları için gerekler periyodik olarak veya gerekleri etkileyecek bir değişiklik olduğunda gözden geçirilmelidir.

4.44.4. Gizlilik ve ifşa etmeme anlaşmaları kurumsal bilgileri korumalı ve imzalayanın, bilginin korunmasından, kullanılmasından ve ifşa edilmesinden yetkili ve sorumlu olduğunu belirtmelidir.

4.44.5. Farklı koşullarda gizlilik ve ifşa etmeme anlaşmaları kuruluşun ihtiyaçtan doğrultusunda farklı şekillerde kullanılmalıdır