1. AMAÇ

Bu politikanın amacı, Konya Teknik Üniversitesinin Bilgi Güvenliği Yönetim Sistemi (BGYS) ile ISO 27001:2022 standartları arasındaki farkları tespit etmek, mevcut durumu anlamak ve bu farkların sistematik bir şekilde analiz edilmesini sağlamaktır.

2. KAPSAM

Bu politika, üniversitenin BGYS ile ISO 27001:2022 standardı arasındaki farkları tespit etmeyi amaçlayan GAP analiz sürecini kapsar. Bu politika, sadece farkların belirlenmesi sürecini içerir; iyileştirme planları, risk analizleri veya risk değerlendirme süreçlerini kapsamaz fakat GAP analizinin çıktısı bu süreçlerin girdisi olarak işlev görür.

3. DAYANAK

Bu politikanın temel dayanağı TS ISO/IEC ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YÖNERGESİ ve ilgili diğer mevzuattır.

4. TANIMLAR

BİDB: Bilgi İşlem Daire Başkanlığı.
Üniversite: Konya Teknik Üniversitesi
GAP Analizi: Mevcut sistemin hedeflenen standartlara göre eksiklerini ve farklılıklarını tespit eden analiz süreci.
BGYS: Bilgi Güvenliği Yönetim Sistemi, üniversitenin bilgi güvenliği yönetimi süreçlerini kapsar.
ISO 27001: Bilgi güvenliği yönetimi için uluslararası bir standart.
Eksiklik (GAP): Mevcut sistemin ISO 27001 gerekliliklerine tam olarak uymadığı noktalar.

5. SORUMLULAR

BİDB: Bu politikanın hazırlanmasından ve uygulanmasından BİDB sorumludur.
BGYS Yönetim Temsilcisi: GAP analizi sürecini koordine eder ve raporların düzenli olarak oluşturulmasını sağlar.
GAP Analiz Ekibi: Analiz sürecini yürüten uzman ekip, BGYS Yönetim Temsilcisi tarafından atanır.
BGYS Komisyonu(Üst Yönetim): GAP analiz sonuçlarını gözden geçirir ve değerlendirir.

6. UYGULAMA

6.1. Planlama

6.1.1. Zaman Çizelgesi: GAP analizleri düzenli aralıklarla yapılır (minimum yılda bir kez yapılır, büyük değişikliklerden sonra da yapılır).

6.1.2. Ekiplerin Belirlenmesi: GAP analizine katılacak ekipler ve ilgili departmanlar belirlenir.

6.1.3. Analiz Kapsamı: GAP analizi kapsamında incelenecek alanlar belirlenir. ISO 27001:2022 gerekliliklerine göre incelenecek maddeler ve BGYS'nin hangi alanlarının analiz edileceği tanımlanır.

6.1.4. İlgili Dokümanların Toplanması: Analiz için gereken mevcut BGYS dokümanları, prosedürler, politikalar ve uygulamalara dair dökümantasyon toplanır.

6.2. Mevcut Durumun Tespiti (Durum Analizi): Üniversitenin mevcut BGYS'si kapsamlı bir şekilde analiz edilmelidir. Bu, aşağıdaki yöntemlerle yapılabilir:

6.2.1. Belge İncelemeleri: Mevcut politikalar, prosedürler, talimatlar ve uygulama planları dikkatlice incelenir .

6.2.2. İlgili Birimlerle Görüşmeler: Uygulamada olan bilgi güvenliği süreçleri ve kullanılan teknolojiler yetkili kişilerle değerlendirilir. İlgili departmanlar ve personel ile görüşmeler yapılır. Bilgi güvenliği süreçlerinin nasıl uygulandığı incelenir.

6.2.3. Saha İncelemeleri: Sistemler ve süreçler yerinde değerlendirilir. Uygulamadaki bilgi güvenliği önlemleri ve teknolojilerinin mevcut durumu gözden geçirilir.

6.3. Standartlarla Karşılaştırma: Mevcut BGYS dokümantasyonunun ve uygulamalarının ISO 27001:2022 standardı ile sistematik olarak karşılaştırması yapılır. Bu aşamada şunlara dikkat edilmelidir:

6.3.1. Standart Gereksinimlerin Karşılaştırılması: Mevcut BGYS, ISO 27001:2022 gereklilikleri ile karşılaştırılır ve eksiklikler belirlenir.

6.3.2. Eksikliklerin Kayıt Altına Alınması: Tespit edilen her eksiklik ayrıntılı bir şekilde not edilir.

6.4. Eksikliklerin ve Farkların Belirlenmesi: GAP'lar, yani eksiklikler ve farklar net bir şekilde tanımlanmalıdır. Bu farklar aşağıdaki türlerde olabilir:

6.4.1. Dokümantasyon Eksiklikleri: Mevcut politikaların veya prosedürlerin ISO 27001 gereksinimlerine uygun olmaması.

6.4.2. Uygulama Eksiklikleri: Belirli bilgi güvenliği kontrollerinin uygulanmaması veya yetersiz uygulanması.

6.4.3. Teknolojik Eksiklikler: Bilgi güvenliği teknolojilerinin yeterli seviyede olmaması.

6.5. Eksikliklerin Sınıflandırılması ve Önceliklendirilmesi: Tespit edilen eksiklikler, öncelik sırasına göre sınıflandırılmalıdır:

6.5.1. Kritik Eksiklikler: Bilgi güvenliği açısından ciddi risk oluşturan ve hemen ele alınması gereken eksiklikler. ("Yüksek" ve "Çok Yüksek" olarak ikiye ayrılabilir)

6.5.2. Orta Düzey Eksiklikler: İyileştirilmesi gereken, ancak acil olmayan eksiklikler.

6.5.3. Düşük Düzey Eksiklikler: İzlenmesi gereken, ancak bilgi güvenliği üzerinde doğrudan büyük bir etkisi olmayan küçük eksiklikler. ("Düşük" ve "Çok Düşük" olarak ikiye ayrılabilir.)

6.6. Rapor Hazırlanması

GAP analizi, kapsamlı bir raporla sonuçlanmalıdır. Bu raporda şunlar yer almalıdır:

6.6.1. GAP Analizi Metodolojisi: Analizin nasıl yapıldığına dair detaylı bilgi. GAP analizi kapsamı ve yöntemi.

6.6.2. Eksikliklerin Detaylı Listesi: Belirlenen tüm eksiklikler ve farklar, ISO 27001 standardının hangi maddesine uygun olmadıklarıyla birlikte belirtilmelidir.

6.6.3. Eksikliklerin Önceliklendirilmesi: Her eksikliğin önemi ve aciliyet derecesi net olarak tanımlanmalıdır.

6.6.4. Sonuç ve Öneriler: GAP analizinin sonucunda alınabilecek aksiyonlar hakkında öneriler sunulmalıdır (iyileştirme planlarına yön vermek amacıyla).

6.7. Rapor Sunumu

GAP Analiz Raporu, tespit edilen farklar, analiz kapsamı ve detaylı bulgular bir rapor halinde BGYS Yönetim Temsilcisi tarafından üst yönetime sunulur ve değerlendirme süreci başlatılır.

6.8. Dokümantasyon

6.8.1. GAP analiz sonuçları ve raporları üniversitenin BGYS dokümantasyon sisteminde saklanır.

6.8.2. Tüm bulgular ve analiz sonuçları, ileride yapılacak gözden geçirmeler için kayıt altına alınır.

7. GÖZDEN GEÇİRME VE REVİZYON

Bu politika, her GAP analizinden sonra gözden geçirilir ve gerektiğinde güncellenir. Ayrıca, organizasyondaki önemli değişiklikler veya ISO 27001 standardındaki güncellemeler dikkate alınarak revizyon yapılır.

8. YAPTIRIM

Bu politikanın ihlal edilmesi durumunda KTÜN BİLGİ GÜVENLİĞİ POLİTİKASI'nda belirtilen "POLİTİKANIN İHLALİ VE YAPTIRIMLAR" başlığı altındakiler geçerlidir.

9. YÜRÜRLÜK

Bu politika, Konya Teknik Üniversitesi Bilgi İşlem Daire Başkanlığının web sayfasında yayımlanarak duyurusu yapıldığı tarihte yürürlüğe girer.

10. YÜRÜTME

Bu politika, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.