AMAÇ

KTÜN BGYS Hedefleri, üniversitenin bilgi güvenliği ihtiyaçlarını karşılarken, aynı zamanda öğrenci ve akademik personelin ihtiyaçlarına uygun bir güvenlik kültürü oluşturmayı amaçlamaktadır.

YÖNTEM

KTÜN BGYS Hedefleri, ISO 27001:2022 standardı dikkate alınarak hazırlanmıştır.

ISO 27001:2022'de BGYS hedeflerine ilişkin gereklilikler, **Madde 6.2 – Bilgi Güvenliği Hedefleri ve Planlaması** başlığı altında aşağıdaki şekilde yer almaktadır:

"Bilgi güvenliği gereksinimlerini, risk değerlendirmesi ve risk işleme sonuçlarını dikkate alarak, uygulanabilir (ve mümkünse ölçülebilir) bilgi güvenliği hedefleri oluşturun. Ne yapılacağını, hangi kaynakların gerektiğini, kimlerin sorumlu olacağını, ne zaman tamamlanacağını ve sonuçların nasıl değerlendirileceğini belirleyin."

Bu madde, SMART (Specific, Measurable, Achievable, Relevant, Time-bound) Prensiplerine uygun olarak hedeflerin aşağıdaki şekilde belirlenmesini öngörür:

1. **Uyumlu Olmak:** Hedeflerin bilgi güvenliği politikasına uygun olması ve risk değerlendirmesine dayalı olarak belirlenmesi gerekir.
2. **Ölçülebilir Olmak:** Hedeflerin konuya özgü spesifik ve ölçülebilir (mümkünse) olması gerekir.
3. **İzlenebilir ve Gözden Geçirilebilir Olmak:** Hedeflerin düzenli olarak gözden geçirilmesi, gerektiğinde güncellenmesi gereklidir.
4. **Belirli Bir Süreç ve Plan Dahilinde:** Hedeflere ulaşmak için hangi süreçlerin izleneceği ve hangi kaynakların kullanılacağı, kimlerin sorumlu olacağı ve ne zaman tamamlanacağı ve sonuçların nasıl değerlendirileceği belirlenmelidir.

HEDEFLER

1. **Bilgi Varlıklarının Korunması:**
    a. Üniversite içinde üretilen, kullanılan ve saklanan her türlü akademik, idari ve araştırma verilerinin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak.
    b. Öğrenci, akademisyen ve personel bilgilerinin korunmasına yönelik güvenlik kontrollerini geliştirmek ve sürekli gözden geçirmek.
    c. Hassas verilerin gizliliğini sağlamak için tüm sistemlerde veri şifreleme oranını %100'e çıkarmak.
    d. Tüm bilgi varlıklarının %100'ü için sahiplik ve sınıflandırma çalışmalarını tamamlamak.

2. **Akademik ve Araştırma Verilerinin Güvenliği:**
    a. Öğrenci ve öğretim üyelerinin akademik bilgilerini (notlar, projeler, araştırmalar vb.) yetkisiz erişimlerden koruyarak akademik süreci güvence altına almak.
    b. Üniversite araştırma projeleri sırasında toplanan ve üretilen hassas verilerin korunması, yetkisiz kişilerle paylaşılmasının önlenmesi ve sadece yetkili kişilere erişim sağlanması.
    c. Uzaktan eğitim platformları ve diğer dijital öğrenme ortamlarında bilgi güvenliği standartlarını uygulayarak öğrencilerin ve öğretim üyelerinin güvenli erişimini sağlamak.

3. **Yasal ve Düzenleyici Gereksinimlere Uygunluk:**
    a. Bilgi güvenliği ile ilgili yasal, düzenleyici ve üniversite politikalarına tam uyum sağlamak (ör. KVKK, GDPR, telif hakkı yasaları).
    b. Öğrenci, personel ve üçüncü taraflara ait kişisel verilerin yasal düzenlemelere uygun şekilde toplanması, işlenmesi, saklanması ve imhasını sağlamak.
    c. Kişisel veri işleme süreçlerinin KVKK ve GDPR gibi düzenlemelere uygun olmasını sağlamak.
    d. Yılda bir kez düzenleyici ve yasal gereksinimlerle ilgili güncellemeleri gözden geçirmek ve uygulamak.
    e. 2025 yılı itibariyle %100 yasal uyum sağlamak ve düzenleyici kurum denetimlerinden başarıyla geçmek.

4. **ISO-27001 standartlarına Uygunluk:**
    a. 2026 yılı sonuna kadar ISO/IEC 27001:2022 belgesi almak.
    b. Belirlenen kişilerin ISO/IEC 27001:2013 İç Tetkikçi eğitimi almasını sağlamak.
    c. BGYS için yıllık ihtiyaç kadar bütçe ayırmak.
    d. Riskleri minimum düzeye indirmek.

5. **Tedarikçi Güvenliği ve Üçüncü Taraflarla İşbirliği:**
    a. Üniversite ile işbirliği yapan tedarikçilerin ve üçüncü tarafların bilgi güvenliği politikalarına uyumunu sağlamak.
    b. Tedarikçilerle yapılan sözleşmelerin %100'ünde bilgi güvenliği maddelerinin yer almasını sağlamak.
    c. Tedarikçilerin güvenlik açıklarının üniversiteye etkisini minimize etmek için denetim süreçlerini iyileştirmek.
    d. Kritik tedarikçilerin yılda en az bir kez bilgi güvenliği performansını değerlendirmek.

6. **Siber Saldırıların Önlenmesi:**
    a. Üniversite altyapısına yönelik siber saldırılara karşı gerekli güvenlik önlemlerini almak, saldırı durumlarında hızlı müdahale etmek ve etkilerini en aza indirmek.
    b. Güvenlik duvarı, IDS/IPS gibi siber savunma sistemlerinin sürekli güncelliğini sağlamak.
    c. Bilgi sistemlerinde yer alan güvenlik zafiyetlerini tespit edip, gerekli iyileştirmeleri düzenli olarak uygulamak.
    d. 2024 yılı itibariyle penetrasyon testlerinde tespit edilen kritik zafiyetlerin %100'ünü 1 ay içinde gidermek.
    e. Güvenlik yamalarının sistemlere uygulanma sürecini %90 oranında 15 gün içerisinde tamamlamak.

7. **Loglama ve İzleme:**
    a. Üniversitenin bilgi sistemlerinde yapılan tüm erişim ve değişikliklerin kayıt altına alınmasını sağlamak.
    b. Loglama ve izleme faaliyetlerinin belirli periyotlarla gözden geçirilerek güvenlik olaylarına karşı hızlı yanıt verilmesini sağlamak.

8. **Bilgi Güvenliği Olay Yönetimi:**
    a. Bilgi güvenliği olaylarını hızlı bir şekilde tespit etmek, ilgili prosedürler doğrultusunda olaylara müdahale etmek ve tekrarını önleyecek düzeltici faaliyetleri gerçekleştirmek.
    b. 2025 yılı sonuna kadar bilgi güvenliği olaylarının sayısını %20 oranında azaltmak.
    c. Güvenlik olaylarına müdahale süresini 30 dakika içinde başlatacak şekilde optimize etmek.

9. **Bilgi Güvenliği Farkındalığı:**
    a. Tüm personel ve öğrencilerin bilgi güvenliği farkındalığını artıracak eğitim programları düzenlemek ve bilgilendirme faaliyetleri yürütmek.
    b. Tüm çalışanlara yılda en az iki kez bilgi güvenliği farkındalık eğitimi sağlamak.
    c. Çalışanların bilgi güvenliği politikalarına ve prosedürlerine uyum oranını %95'in üzerine çıkarmak.

10. **İş Sürekliliği, Veri Yedekleme ve Kurtarma:**
    a. Üniversitenin tüm kritik verilerinin düzenli olarak yedeklenmesini sağlamak ve olası veri kayıpları durumunda etkin kurtarma prosedürlerini uygulamak.
    b. Üniversitenin kritik bilgi sistemlerinin kesintisiz çalışmasını sağlamak için bir iş sürekliliği ve felaket kurtarma planı geliştirmek, test etmek ve güncellemek.

c. Potansiyel iş kesintilerine yönelik yılda en az bir defa tatbikat yapmak.
d. Üniversitenin uzaktan eğitim sistemlerinde olası kesintilere ve güvenlik tehditlerine karşı hazırlıklı olunmasını sağlamak.
e. Bilgi teknolojileri sistemlerinin %99,9 oranında erişilebilir olmasını sağlamak.
f. Yılda en az bir kez iş sürekliliği ve felaket kurtarma tatbikatı gerçekleştirmek.
g. Bulut tabanlı sistemlerde yedekleme politikalarının güvenliğini denetlemek ve yedeklerin korunmasını sağlamak.

11. **Mobil ve Taşınabilir Cihaz Güvenliği:**
    a. Üniversite tarafından sağlanan veya kişisel taşınabilir cihazlarla üniversite ağına erişen kullanıcılar için güvenlik politikalarının uygulanmasını sağlamak.

12. **İç ve Dış Denetimlerin Yürütülmesi:**
    a. BGYS'nin etkinliğini ve uyumluluğunu değerlendirmek için düzenli olarak iç ve dış denetimlerin yapılmasını sağlamak.
    b. Yılda en az bir iç bilgi güvenliği denetimi gerçekleştirmek.
    c. Güvenlik denetimlerinden elde edilen uygunsuzlukların %100'ünü 3 ay içerisinde düzeltmek.

13. **Ölçme ve Değerlendirme:**
    a. Bilgi güvenliği hedeflerinin performansını düzenli olarak ölçmek, sonuçları analiz etmek ve iyileştirme süreçleri geliştirmek.
    b. BGYS hedefleri, belirlenen performans göstergeleriyle yılda en az bir kez yönetim gözden geçirme toplantılarında değerlendirmek.
    c. İç ve dış denetimlerle bilgi güvenliği yönetim sisteminin etkinliğini değerlendirmek.
    d. Hedefler, KTÜN'ün bilgi güvenliği stratejisine, risk yönetimi süreçlerine ve iş hedeflerine uygun olarak revize etmek.