TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

BİLGİ GÜVENLİĞİ
POLİTİKASI

Revizyon Takibi:

Sıra No	Rev. No	Tarih	Hazırlayan	Revizyon Nedeni	Onaylayan	İmza
1						
2						
3						
4						

1. AMAÇ

TS EN ISO 27001:2022 Bilgi Güvenliği Politikasının amacı Türk Alman Üniversitesi Bilgi İşlem Daire Başkanlığına ait; insan, altyapı, yazılım, donanım, kullanıcı bilgileri, kurum bilgileri, üçüncü şahıs bilgileri ve finansal kaynaklar için bilgi güvenliği yönetiminin sağlandığını göstermek; risk yönetimini güvence altına almak; bilgi güvenliği yönetimi süreç performansını ölçmek ve bilgi güvenliği ile ilgili konularda üçüncü taraflarla olan ilişkilerin düzenlenmesini sağlamaktır. Ayrıca, her türlü siber saldırı, veri kaybı ve güvenlik ihlallerinin önüne geçilmesi hedeflenmektedir.

2. KAPSAM

Bu politika, Türk Alman Üniversitesi'nin sorumluluğunda olan tüm bilgi sistemlerini, cihazlarını, veri tabanlarını, ağ altyapısını ve uygulama yazılımlarını kapsar. Ayrıca üniversite içindeki tüm akademik ve idari personel, öğrenciler ve misafir kullanıcıları da kapsamaktadır.

3. SORUMLULUK

Bilgi güvenliğinin yönetiminden, denetiminden, politikaların oluşturulmasından ve onaylanmasından Bilgi Güvenliği Ekibi sorumludur. Bilgi Güvenliği Politikasının uygulanmasından Türk Alman Üniversitesi personelleri ve gerektiğinde üçüncü şahıslar sorumludur.

4. UYGULAMA

4.1. Temel İlkeler

- **Gizlilik:** Üniversiteye ait her türlü bilgi ve veri, yalnızca yetkili kişiler tarafından erişilebilecektir. Bilgilerin gizliliği korunacak ve yetkisiz erişime karşı önlemler alınacaktır.
- **Bütünlük:** Üniversite bilgileri, değişikliklere karşı korunacak ve sadece yetkili kişiler tarafından güncellenebilecektir. Veri bütünlüğü sağlanarak, yanlışlıkla ya da kötü niyetli değişikliklerin önüne geçilecektir.
- **Erişilebilirlik:** Üniversite sistemlerine yetkili kişiler tarafından her zaman erişim sağlanabilmelidir. Sistemlerin sürekli çalışabilirliği ve veri kaybı riskinin en aza indirilmesi sağlanacaktır.

4.2. Güvenlik Yöntemleri

- **Erişim Kontrolü:** Bilgi sistemlerine erişim yalnızca yetkili kullanıcılarla sınırlıdır. Kullanıcıların sistemlere erişim seviyeleri belirli kriterlere göre sınıflandırılacak ve en düşük yetki prensibine dayanarak düzenlenecektir.
- **Şifre Güvenliği:** Kullanıcı şifreleri güçlü ve karmaşık olacak şekilde belirlenmelidir. Şifreler düzenli aralıklarla değiştirilmelidir. Şifrelerin üçüncü şahıslarla paylaşılması yasaktır.

- **Ağ Güvenliği:** Üniversitenin ağ altyapısı, dış tehditlere karşı güvenlik duvarları, anti virüs yazılımları ve diğer güvenlik önlemleriyle korunacaktır. Ağda tespit edilen her türlü şüpheli etkinlik derhal izlenecek ve gerekli önlemler alınacaktır.

- **Veri Yedekleme:** Kritik veriler düzenli aralıklarla yedeklenecek ve yedekler güvenli bir şekilde saklanacaktır. Yedekleme sistemlerinin güvenliği de sağlanacaktır.

- **Fiziksel Güvenlik:** Bilgi işlem altyapısının bulunduğu fiziksel alanlar, yalnızca yetkili kişilerin erişebileceği şekilde güvence altına alınacaktır. Sunucular, ağ cihazları ve diğer kritik donanımlar güvenli bir ortamda bulundurulacaktır. Sadece elektronik ortamda tutulan verilerin değil; yazılı, basılı, sözlü ve benzeri tüm verilerin güvenliği sağlanacaktır.

4.3. Kullanıcı Eğitimi ve Farkındalık

Türk Alman Üniversitesi, bilgi güvenliği kültürünü yaygınlaştırmak amacıyla tüm kullanıcılar için düzenli olarak eğitimler vererek, güvenlik tehditleri ve korunma yöntemleri konusunda farkındalık yaratacaktır. Bu eğitimler, çalışanlar, öğrenciler ve diğer üniversite kullanıcıları için zorunlu olacaktır.

4.4. Bilgi Güvenliği İhlalleri ve Olay Yönetimi

Bilgi güvenliği ihlalleri tespit edildiğinde, olay yönetim süreci devreye girecek ve ihlalin türüne göre gerekli adımlar atılacaktır. Olay yönetim süreci aşağıdaki aşamalardan oluşacaktır:

- **Tespit:** Olayın fark edilmesi ve kayda alınması.

- **İzleme ve Analiz:** Olayın detaylı şekilde analiz edilmesi.

- **Yanıt:** Olayın etkilerini minimize etmek için alınacak aksiyonlar.

- **İyileştirme:** Olay sonrası süreçlerin iyileştirilmesi ve gelecekte benzer ihlallerin önlenmesi.

4.5. Yasal Yükümlülükler ve Düzenlemeler

Türk Alman Üniversitesi, ulusal ve uluslararası bilgi güvenliği yasalarına ve düzenlemelere tam uyum sağlamayı taahhüt eder. Ayrıca, kullanıcı bilgileri ve verilerinin korunması konusunda veri koruma yönetmeliklerine uygun hareket edilecektir.

4.6. Politika Denetimi ve Güncellemeler

Bu politika, belirli aralıklarla gözden geçirilecek ve güncellenecektir. Ayrıca, güvenlik tehditlerinde yaşanacak değişiklikler doğrultusunda hızla revize edilecektir. BGYS Ekibi İş sürekliliği planları hazırlar ve test eder.

5. YAPTIRIM

Bu politikaya uygun olarak çalışmayan tüm personel hakkında ilgili personel kanununun hükümleri uygulanır.

6. İLGİLİ DOKÜMANLAR

ISO/IEC 27001:2022