1. AMAÇ

Bu politika, Hakkari Üniversitesi güvenli yazılım geliştirme süreçlerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesini amaçlamaktadır.

2. KAPSAM

Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında Hakkari Üniversitesi bünyesinde kullanılan ve geliştirilen yazılımları kapsar.

3. TANIMLAR VE KISALTMALAR

BGYS: Bilgi Güvenliği Yönetim Sistemi'nin kısaltmasıdır.

Bilgi Güvenliği Yönetim Sistemi: Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, risk yaklaşımına dayalı yönetim sistemidir.

Yazılım Geliştirme: Kullanıcı ihtiyaçlarına yönelik yazılım çözümleri üretmek için yapılan analiz, tasarım, kodlama, test etme ve bakım faaliyetlerini ifade eder.

Yazılım: Bilgisayarların ve diğer dijital cihazların belirli görevleri yerine getirmesini sağlayan, kodlanmış talimatlar ve veriler bütünüdür.

4. SORUMLULUKLAR

Bilgi Güvenliği Yönetim Sistemi Komisyonu: Bu politikanın hazırlanmasından ve güncellenmesinden sorumludur.

Bilgi İşlem Daire Başkanı: Politikanın kontrolü ve uygulanabilirliğinin sağlanmasından sorumludur.

Rektör: Politikanın onaylanması ve yürürlüğe konulmasından sorumludur.

İlgili Personel: Politika içinde belirtilen faaliyetlerin gerçekleştirilmesinden sorumludur.

5. UYGULAMA

a) Bilgi İşlem Daire Başkanı sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.

b) Uygulama yazılımlarının Üniversite içerisinde mi hazırlanacağı yoksa satın mı alınacağının belirlenmesi, uygun bir şekilde tanımlanmalıdır.

c) Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir iş planı kullanılmalıdır.

d) Üniversite içinde geliştirilmiş yazılımlar ve seçilen paket sistemler, ihtiyaçları karşılamalıdır.

e) Yazılım geliştirme politikalarına uygun olmayan, ulusal ve uluslararası yazılım geliştirme standartları çerçevesinde geliştirilmemiş ve Üniversite talebi olmaksızın üretilmiş olan yazılımların Üniversite sistemler üzerine entegre edilmesine izin verilmemelidir.

f) Hazırlanan sistemler mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları ilgili personele e-posta ile bilgilendirmesi yapılmalıdır.

g) Yeni alınmış veya revize edilmiş bütün yazılımlar test ortamında kontrol edilmelidir. Herhangi bir sorun görülmesi durumunda üretici firma ile iletişime geçilip çözüm arayışına girilir.

h) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

i) Yazılımlar sınıflandırılmalı ve envanterleri çıkarılarak varlık envanterinde güncellenmelidir.

j) Üniversitede kişisel olarak geliştirilmiş yazılımların kullanılması engellenmelidir.

k) Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.

l) Politika ihlali disiplin kurallarına tabi olmanıza neden olabilir ve yasal sonuçlar doğabilir.