İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

TEKNİK AÇIKLIK YÖNETİM POLİTİKASI (TAYP)

HAZIRLAYANLAR	KONTROL EDEN	ONAYLAYAN
Ufuk Dikme	İsmail Koç	
Bilgi Güvenliği Yönetim Müdürü	Bilgi Sistemleri ve Teknolojileri Daire Başkanı	Rektörlük Temsilcisi

İÇİNDEKİLER

1. AMAÇ

Bu politika, T.C. İstanbul Kültür Üniversitesi bünyesinde kullanılmakta olan bilgi sistemlerinin teknik açıklıklarına dair ortaya çıkabilecek riskleri ele almak, zafiyetleri değerlendirmek ve uygun tedbirleri almak amacıyla gerekli olan şartları tanımlamak için hazırlanmıştır.

2. KAPSAM

Bu politika, T.C. İstanbul Kültür Üniversitesi bünyesindeki tüm sistemleri kapsamaktadır.

3. DAYANAK

- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin Ek.A.12.6.1 maddesi.
- 15.03.2018 tarihli ve 19924119-719-E.21240 sayılı "2016-2019 Ulusal Siber Güvenlik Eylem Planı" konulu YÖK yazısında, üniversitelerin ISO27001 Bilgi Güvenliği Yönetim Sertifikası alması ve iş süreçlerini bu şekilde yapılandırması gerektiği ifade edilmiştir.

4. TANIMLAR VE KISALTMALAR

KISALTMALAR	TANIMLAR
BSTDB	Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı
İKÜ	T.C. İstanbul Kültür Üniversitesi

5. İLGİLİ DOKÜMANLAR

No	İLGİLİ ARAÇLAR
1	IKU BSTDB Bilgi Güvenliği Disiplin Politikası
2	IKU BSTDB Bilgi Güvenliği İhlal Olayları Prosedürü
3	İKÜ Sızma Testi Teknik Şartnamesi

6. TEKNİK AÇIKLIK YÖNETİM POLİTİKASININ HEDEFLERİ VE PRENSİPLERİ

6.1. Varlıkların güncel ve eksiksiz envanteri etkili teknik açıklıkların yönetilmesi için oluşturulmuştur.

6.2. Bu varlık envanteri, teknik açıklıkların yönetilmesini desteklemek için gerekli özel bilgileri; yazılım tedarikçisini, sürüm numarasını, dağıtımın mevcut durumunu ve yazılım için kuruluş içindeki sorumlu kişiyi/kişileri içerir.

6.3. İKÜ, izleme, açıklık, risk değerlendirmesi, yama, varlık izleme ve her türlü koordinasyon görevleri de dâhil olmak üzere teknik açıklıkların yönetilmesi ile ilişkili BSTDB müdürlerini görevlendirmiştir.

6.4. İlgili teknik güvenlik açıklıklarını belirlemek ve onlar hakkında farkındalığı korumak için BSTDB her yıl en az bir kere olmak üzere sızma testi yaptırır.

6.5. Sızma testi için isterler "İKÜ Sızma Testi Teknik Şartnamesi" içerisinde belirlenmiştir.

6.6. Olası teknik açıklıkların belirlenmesinden sonra BSTDB Bilgi Güvenliği Müdürü riskleri ve alınması gereken eylemleri tanımlar. Bu eylemler risk seviyelerine göre öncelik verilerek çözümler sağlanır.

6.7. Meşru kaynaklarda yayınlana bir yama varsa, yama yükleme ile ilgili riskler değerlendirilir. (Yamanın yüklenmesi riski ile açıklığın oluşturduğu risklerin karşılaştırılması),

6.8. Yamaların, etkinliğinden emin olmak ve geri dönülemez etkilerle sonuçlanmasından kaçınmak için kurulum öncesinde test edilip "IKU BSTDB Değişiklik Yönetimi Prosedürü" kapsamında değerlendirilir. Eğer yama yoksa aşağıdaki kontroller dikkate alınır;

6.8.1. Açıklıkla ilgili hizmetlerin ya da özelliklerin kapatılması.

6.8.2. Erişim kontrollerinin uyumlaştırılması ya da eklenmesi, örneğin; güvenlik duvarları, ağ sınır cihazları.

6.8.3. Gerçek saldırıların tespiti için izlemenin arttırılması.

6.8.4. Güvenlik açığı hakkında farkındalığın arttırılması.

6.9. Gerçekleştirilen tüm prosedürler için bir denetim kaydı tutulur.

6.10. Teknik açıklık yönetim politikasının etkinliğinden ve verimliliğinden emin olmak için politika düzenli olarak izlenir ve değerlendirilir.

6.11. Teknik açıklıklar çalışma saatleri dışında planlanır. Çok acil durumlarda mümkünse en az çalışmanın yapıldığı saat dilimleri seçilir. Çalışma yapılmadan önce ilgili birimlere bilgi verilir.

7. TEKNİK AÇIKLIK YÖNETİM POLİTİKASININ YAPTIRIMLARI

Bu politikanın ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla "IKU BSTDB Bilgi Güvenliği Disiplin Politikası" ve "IKU BSTDB Bilgi Güvenliği İhlal Olayları Prosedürü" belgelerinde belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

8. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar
TAYP-001-1.0		6.11. Teknik açıklıklar çalışma saatleri dışında planlanır. Çok acil durumlarda mümkünse en az çalışmanın yapıldığı saat dilimleri seçilir. Çalışma yapılmadan önce ilgili birimlere bilgi verilir.	Ufuk Dikme