İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

ZARARLI YAZILIMLARDAN KORUNMA POLİTİKASI (ZYKP)

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

Doküman Kod	IKU-BSTDB-ZYKP-001	Revizyon Tarihi	
Yayın Tarihi	07.01.2022	Revizyon No	ZYKP -001-1.0

İÇİNDEKİLER

1. AMAÇ

Bu dokümanın amacı, T.C. İstanbul Kültür Üniversitesinde bilgi işleme olanaklarının güvenli işletimlerini temin etmektir.

Bu amaçla zararlı yazılımlara karşı koruma için kötü amaçlı yazılım tespit ve onarım yazılımı, kullanıcılarda bilgi güvenliği bilinci, uygun sistem erişim ve değişim yönetimi ve yazılım kurulum esaslarına ilişkin kontrolleri bildirmektir.

2. KAPSAM

Bu dokümanın kapsamı, tüm bilgi varlıklarını içerir.

3. DAYANAK

- 5651 numaralı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.
- 6698 numaralı Kişisel Verilerin Korunumu Kanunu
- 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

5. İLGİLİ DOKÜMANLAR

No	İLGİLİ ARAÇLAR

6. YAZILIM KURULUMU VE KÖTÜCÜL YAZILIMLARDAN KORUNMA

6.1. Tüm sistemdeki güvenlik yazılımları çalışması, veritabanı güncelliği ve bulunan virüsler düzenli olarak kontrol edilir.

6.2. Sunucu ve bilgisayarlarda (taşınabilir, masaüstü, kurum tarafından verilen mobil cihazlarda) antivirüs yazılımı yüklü olacaktır.

6.3. Gelen e postalar, eposta sunucusu ile entegre çalışan antivirüs yazılımı ile aktif olarak taranacaktır.

6.4. Kuruluş bilgisayarlarına USB disk, harici disk ya da CD takıldığı zaman kullanıcıda kurulu olan antivirüs yazılımı tarafından taranır.

6.5. Yazılım kurulumlarında, en az ayrıcalık hakkı ya da ihtiyacı kadar hak tanımlama prensibine uygun tanımlanarak düzenlenir.

6.6. Zararlı kod içeren ve/veya kötü amaçlı web siteleri engellenmelidir.

6.7. Kötü amaçlı yazılımların kullanabilecekleri zafiyetlerin tespit edilmesi için yılda en az bir kez teknik güvenlik testleri yapılacaktır.

6.8. Kullanılan anti virüs yazılımı üzerinde düzenli taramalar yapılacak şekilde konfigürasyonlar yapılır.

6.9. Kuruluşun tüm istemcilerinde antivirüs yazılımının çalışıyor ve güncel olmasının sağlanır.

6.10. Kullanıcılara kuruluşa ait bilgisayarda yüklü olan antivirüs yazılımını durdurmamaları konusunda tebliğ yapılır. Kullanıcının kuruluşa ait bilgisayar üzerindeki antivirüs yazılımını durdurması ya da işlevini yerine getirmesini engellemesinin tespiti durumunda "Disiplin Süreci" işletilir.

6.11. Dış kaynaklardan gelen veriler ve/veya yazılımlar antivirüs yazılımı ile kontrol edilmeden kuruluş bilgi sistemlerine dâhil edilmemelidir.

6.12. Sistemde tespit edilen zararlı yazılımlar incelenmeli ve sisteme erişim yolları tespit edilmelidir.

6.13. Zararlı yazılımların temizlenmesi esnasında sistem ve veri bütünlüğünün zarar görmemesine özen gösterilir. Kurtarma işlemlerinden önce yedekleme ve geri dönüş planları yapılır.

6.14. Zararlı yazılımlar için özel ilgi grupları ile kullanılan güvenlik yazılımlarının grupları takip edilir.

6.15. Zararlı yazılımdan etkilenen sistemler izole edilir.

7. ZARARLI YAZILIMLARDAN KORUNMA 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