T.C.
İSTANBUL
KÜLTÜR
ÜNİVERSİTESİ

İKÜ BST

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

UZAKTAN ERİŞİM POLİTİKASI (UEP)

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 Üniversitesinin sahip olduğu bilgisayar ağına uzaktan erişim standartlarının tanımlanması ve uzaktan erişim işleminden kaynaklanabilecek güvenlik açıklarının engellenmesi amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika, T.C. İstanbul Kültür Üniversitesi Ayniyat Birimine kayıtlı, İKÜ kullanımında olan, uzak erişim sağlayabilen tüm cihazlar ve sistemler, uzaktan erişim sağlayan çalışanlar ya da anlaşmalı firma çalışanlarının şahsi cihazları ve bu kişileri kapsamaktadır.

3. DAYANAK

- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin Ek.A.6.2.2 maddesi.
- 5651 numaralı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.
- 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
ANTIVIRUS	Kötücül Yazılımlardan korunma yazılımı
BSTDB	Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı
İKÜ	T.C. İstanbul Kültür Üniversitesi
P2P	Eşten eşe bağlantı, peer-to-peer network ya da P2P olarak tanımlanmaktadır. İki veya daha fazla makina arasında veri kopyası oluşturmak için kullanılan bir network program protokolüdür.
SSL VPN	SSL VPN, modern bir web tarayıcısı kullanılarak yapılan VPN işlemidir. Kullanıcılar herhangi bir ekstra yazılım veya dosyası indirmesine gerek kalmadan kullanım sağlar.
VPN	VPN (Virtual Private Network) iki sistemin uzaktan güvenli şekilde bağlanmasını sağlayan hizmettir. İki sistemi birbirine bir tünel üzerinden bağlarken veriyi de şifreler.

5. İLGİLİ DOKÜMANLAR

No	İLGİLİ ARAÇLAR
1	IKU BSTDB Bilgi Güvenliği Disiplin Politikası
2	IKU BSTDB Bilgi Güvenliği İhlal Olayları Prosedürü
3	IKU BSTDB Internet Kullanım Politikası
4	IKU BSTDB Uzaktan Çalışma Prosedürü

6. UZAKTAN ERİŞİM POLİTİKASININ HEDEFLERİ VE PRENSİPLERİ

6.1. İKÜ çalışanları ve yetkilendirilmiş firma çalışanları İKÜ bilgisayar ağına ve bilgi kaynaklarına SSL VPN bağlantısı kurarak erişim sağlar.

6.2. İKÜ çalışanları ve yetkilendirilmiş firma çalışanları için tahsis edilen uzaktan bağlantı kaynak ve hizmetleri "IKU BSTDB Internet Kullanım Politikası" çerçevesinde kullanılır.

6.3. Uzaktan erişim hizmeti kişiye özeldir, başka bir kullanıcıya devredilemez. Hizmet alan kullanıcılar bağlantı yaptıkları cihazdan ve bu cihazla yapılan her türlü kural dışı hareketten sorumludurlar.

6.4. İKÜ bilgisayar ağı yatırımları, akademik, idari, eğitim ve araştırma gibi birincil amaçlarına hizmet etmek üzere yapılmaktadır. Uzaktan erişim hizmeti üzerinden kişisel kullanımlar hiçbir zaman diğer kullanıcıların birincil ağ erişim gereksinimlerini (akademik, idari, eğitim, araştırma) yerine getirmelerine engel olmamalıdır.

6.5. İKÜ uzaktan erişim altyapısında kullanılan protokol ve servis standartlarında oluşabilecek herhangi bir zafiyet ve açıklık sebebiyle İKÜ BSTDB sorumlu tutulamaz. İKÜ BSTDB bu tür açıkları en kısa sürede gidermek ile yükümlüdür.

6.6. Kullanıcı, bakım çalışması amacı ile planlı olarak ya da sistem aksaklıkları sebebi ile uzaktan erişim hizmetinde beklenmedik kesintiler yaşayabilir.

6.7. İKÜ BSTDB, kullanıcının uzaktan erişim hizmetini kullanması esnasında herhangi bir hız garantisi vermez.

6.8. İKÜ BSTDB, uzaktan erişim hızını kısıtlamamakla birlikte adil kullanım koşulları çerçevesinde hızın kısıtlanması ve kota uygulanması hakkını elinde tutar.

6.9. İKÜ bilgisayar ağına uzaktan bağlantı yetkisi verilen çalışanlar veya yetkilendirilmiş firma çalışanları bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

6.10. İKÜ bilgisayar ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti-virüs yazılımlarında güncellemeler yapılmış olmalıdır.

6.11. İKÜ ile ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri, yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

6.12. Fiziksel güvenliği olmayan ortamlarda İKÜ BSTDB personeli uzaktan çalışma yapamaz.

6.13. İKÜ'nün iç sistemlerine uzaktan erişim ihtiyacı, erişilecek ve haberleşme hattından geçirilecek bilginin hassasiyeti ve dâhili sistemin hassaslığı dikkate alınarak haberleşme güvenlik gereksinimleri BSTDB personeli tarafından sağlanır.

6.14. İKÜ personelinin ev ağının güvenli yapılandırılmış olması gerekmektedir.

6.15. Uzak çalışma esnasınada kullanılan cihazlar personelin kendisine ait bile olsa üretilen bilgi kurumun bilgisidir.

6.16. İKÜ 'nün kontrolü altında olmayan özel mülkiyete ait teçhizat kullanımının yasak olduğu yerlerde uzaktan çalışma faaliyetleri için uygun donanım ve depolama mobilyaları İKÜ tarafından sağlanır.

6.17. İzin verilmiş işin bir tarifi, iş saatleri, tutulan bilginin sınıflandırılması ve uzaktan çalışan kişinin erişim yetkisi olan iç sistemler ve hizmetler "IKU BSTDB Uzaktan Çalışma Prosedürü" dokümanında tanımlanmıştır.

6.18. Uzaktan erişimi güvenli kılmak için yöntemleri de içeren uygun haberleşme teçhizatlarının kullanılmasına izin verilmektedir.

6.19. BSTDB tarafından uygun görülen minimum özelliklere sahip cihazlar ve yazılımların, uzaktan erişim esnasında, donanım ve yazılım desteği BSTDB Destek Grubu tarafından sağlanır.

6.20. İKÜ sistemlerine uzaktan erişim sağlayan her donanımın izleri tutulur.

7. UZAKTAN ERİŞİM POLİTİKASININ İHLAL DURUMLARI

7.1. P2P dosya paylaşım programlarının kullanılması yasaktır. Uzaktan erişim kullanıcısı bu uygulamaları sisteme bağlanmadan önce kapatmalıdır. Bu tür uygulamaların otomatik açılmasına izin vermemelidir.

7.2. Uzaktan erişim hizmetinin şahsi kazanç ve kâr amacı ile kullanılması yasaktır.

7.3. Uzaktan erişim hizmeti kullanılarak, kitlesel e-posta gönderilmesi ve üçüncü şahısların göndermesine olanak sağlanması yasaktır. Uzaktan erişim kullanıcısı, sisteme bağlanmadan önce virüs taraması yapmalıdır.

7.4. Lisanssız yazılım, film ve müzik dosyaları uzaktan erişim üzerinden herhangi bir yöntemle dağıtılamaz. Bu konu ile ilgili bütün yasal sorumluluk kullanıcıya aittir.

7.5. Ağ güvenliğini tehdit edici faaliyetlerde bulunmak yasaktır.

7.6. Uzaktan erişim hizmetinden faydalanan her kullanıcı, İKÜ tarafından kendisine tahsis edilen kaynakların kullanımından, güvenliğinden ve bu kaynakların bilinçli veya bilinçsiz olarak üçüncü kişilere kullandırılması durumunda ortaya çıkabilecek yasaklanmış faaliyetlerden birinci derecede sorumludur.

7.7. Uzaktan erişim kaynakları üzerinden herhangi bir servis (Proxy, DHCP, BOOTP, DNS vb.) verilemez, herhangi bir yönlendirme protokolü anonsu yapılamaz.

7.8. Uzaktan erişim kullanıcılarının, bu servisten yararlanırken kullandıkları cihazlarda, güvenlik ve teknik desteği devam eden işletim sistemi kullanmaları (Ör: Windows XP, 7 cihazları için güvenlik ve teknik destek Microsoft tarafından sonlandırılmıştır.) ve kendi cihazlarının işletim sistemi, antivirüs ve güvenlik güncellemeleri ve yamalarını yapmaları zorunludur. İKÜ BSTDB, bir kullanıcının Uzaktan erişim bağlantısına izin vermeden önce cihazın güvenlik kontrolünü yapabilir. Yukarıda belirtilen koşullara uyulmaması

durumunda, kullanıcıdan izin alınmaksızın ve aranan güvenlik koşullarına uyulana dek, kullanıcının erişim hizmeti kesilebilir.

8. UZAKTAN ERİŞİM 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.

9. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar