TÜRK-ALMAN ÜNİVERSİTESİ

UZAKTAN ERİŞİM VE ÇALIŞMA POLİTİKASI

Revizyon Takibi:

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

1. AMAÇ

Bu politikanın amacı, Türk-Alman Üniversitesi bilgi sistemlerine uzaktan erişim süreçlerinin yönetimi ve kullanımına ilişkin kuralların belirlenmesidir. Politika, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi 3.1.14.1, 3.1.14.7 maddelerine dayalı güvenlik tedbirlerine uygunluğu hedeflemektedir.

2. KAPSAM

Bu politika, Türk-Alman Üniversitesi bünyesindeki tüm çalışanları ve kullanılan tüm sosyal medya bilgi sistemlerini kapsar.

3. SORUMLULUK

Bu prosedürün uygulanmasından Yönetim Temsilcisi başta olmak üzere tüm personel sorumludur.

4. UYGULAMA

04.1. Uzaktan Erişim Politikasının Hedefleri ve Prensipleri

04.1.1. İnternet üzerinden Türk-Alman Üniversitesi'nin herhangi bir yerindeki bilgisayar ağına uzaktan erişen personel VPN/ZTNA teknolojisini kullanmalıdır. Bu veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığının sağlanması için gereklidir. VPN/ZTNA teknolojisi güvenli protokolleri içermelidir.

04.1.2. Uzaktan erişim güvenliği denetlenmelidir. Uzak bağlantı log kayıtları bütünlüğü korunak saklanmalıdır.

04.1.3. Uzak bağlantı yapmasına izin verilen kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

04.1.4. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

04.1.5. Mobil Telefon hatları ile uzaktan bağlantı yalnızca kurum tarafından sağlanan ve yapılandırma ayarları kurumun bilgi güvenliği gereksinimlerine uygun olan cihazlar ile sınırlandırılmadır.

04.1.6. Uzaktan çalışma kapsamında kurum bilgilerinin işleneceği cihazlarda zararlı yazılımlardan korunma uygulaması bulunmalı ve zararlı yazılımdan korunma uygulamasının en güncel yama dosyaları yüklenmeli, imza veri tabanı güncel olmalıdır.

04.1.7. Uzaktan çalışma kapsamında kurum kaynaklarına erişim VPN/ZTNA teknolojisinin yanı sıra çok faktörlü kimlik doğrulama ile sağlanmalıdır. Erişimler en az yetki prensibine göre tanımlanmalıdır.

04.1.8. Uzaktan çalışma kapsamında kurum bilgilerinin işleneceği cihazların işletim sistemlerinin ve kullanılan uygulamaların güncel olması sağlanmalı, güvenlik yamaları yüklü olmalıdır.

04.1.9. Uzaktan çalışma kapsamında kurumun politikalarına uygun güçlü parolaların kullanılması sağlanmalıdır.

04.1.10. VPN/ZTNA kullanım hakkı verilen kullanıcılar firewall üzerinde listelenmeli ve düzenli olarak kontrol edilmelidir.

04.1.11. Sadece kurumun onay verdiği kullanıcılar VPN/ZNTA kullanabilir.

04.1.12. Kurum personeli dışında üçüncü taraflara verilecek erişimler için gizlilik anlaşması yapılmış olmalıdır.

04.1.13. Kurum personeli dışındaki 3.taraflara Bilgi İşlem Daire Başkanının onayı ile sınırlı süre ile erişim izni verilir.

04.1.14. Uzaktan çalışan kullanıcı bilgisayarlarında olası veri sızıntısını engellemek amacıyla uç nokta seviyesinde veri sızıntısı önlemeye yönelik güvenlik önlemleri alınmalıdır.

04.2. Uzaktan Erişim Politikasının İhlal Durumları

04.2.1. Uzaktan erişimde ağ güvenliğini tehdit edici faaliyetlerde bulunmak yasaktır.

04.2.2. Uzaktan erişim hizmetinin şahsi amaçlar için kullanılması yasaktır.

04.2.3. Uzaktan erişim bilgilerinin korunması konusunda yasal sorumluluk kullanıcıya aittir.

04.2.4. Uzaktan erişimde güvenlik yazılımlarını güncel tutmak zorunludur.

04.2.5. Yukarıda belirtilen koşullara uyulmamasının tespiti durumunda, kullanıcıdan izin alınmaksızın ve aranan güvenlik koşullarına uyulana dek, kullanıcının uzaktan erişim hizmeti kesilebilir.

EK:

TAU-FRM-116-01 UZAKTAN ERİŞİM KULLANICI TALEP FORMU