1. **AMAÇ – KAPSAM :** Başkanlığımız bünyesindeki sunuculara diş paydaşlarca(firma, kamu kurumu) yapılan uzaktan erişimler de yetkisiz kullanımından dolayı, kritik sistemlerde meydana gelebilecek zararları, hassas bilgilerin kaybı ve prestij kaybını önlemek amacıyla Başkanlığımız sunucularına uzaktan erişim yoluyla yapılacak bağlantıların standartları ile başkanlığımız bünyesindeki sunucuların güvenliği açısından standartları tanımlamaktır.

2. **SORUMLULAR :** Bu prosedürün oluşturulmasından ve uygulanmasından Sistem, İdari ve Mali Hizmetler Birimi sorumludur.

3. **UYGULAMA**

3.1. Genel Kurallar

3.1.1. Uzaktan erişim için yetkilendirilmiş kullanıcılar için internet çıkış IP leri güvenlik duvarında tanımlanır. Bu tanımlanan IP lerle erişim sağlanır. Yerel ağdan bağlanan kullanıcılar yetkili kullanıcı adı ve şifresiyle erişim sağlar.

3.1.2. Başkanlığımızda tüm çalışanlar VPN'i kullanabilir, VPN kullanım hakkı verilen çalışanlar yetkisiz kişilere bu hakkı kullandırmaması için gerekli tedbirleri almakla sorumludur.

3.1.3. Uzaktan erişim trafiği sıkı bir şekilde kontrol edilmelidir. Daha fazla bilgi için Şifreleme Prosedürü'ne bakınız.

3.1.4. Başkanlık personelimiz, kurumun hiçbir bilgisini (idari, mali vb.) kurum dışına çıkartamaz. Aksi taktirde oluşacak yasal yükümlülüklerden Bilgi işlem Daire Başkanlığı sorumlu olacaktır.

3.1.5. Başkanlık çalışanları hiç bir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye vermemelidir.

3.1.6. Üniversite ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme yapılmış firmalar bağlantı esnasında aynı anda başka bir ağa bağlı (split tunnel- aynı anda iki vpn bağlantısı) olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.

3.1.7. Uzaktan erişim yöntemi ile Üniversite ağına erişen bütün bilgisayarlar en son güncellenmiş anti-virus yazılımına sahip olmalıdırlar.

3.1.8. Periyodik olarak yapılan kontrollerle Bilgi işlem Daire Başkanlığı ile ilişiği kesilmiş veya görevi değişmiş kullanıcıların hesapları kaldırılmalıdır.

3.1.9. Üniversitemize ait olmayan bilgisayarlara sahip kullanıcılar da kurumumuzun VPN ve Ağ politikalarına uygun bir şekilde cihazlarını konfigre etmelidirler.

3.1.10. İş sürekliliği ve acil durum planlaması için iletişim yöntemleri tanımlanır ve yazılı hale getirilir. Acil durumlarda erişilmesi gereken kişilerin irtibat numaraları ilgili personelin kolayca ulaşabileceği bir şekilde bulundurulur.

3.1.11. Yeni teknolojileri, uygulamaları, tehdit veya açıklıkları takip etmek için dernek, forum siteleri, e-Posta grupları gibi özel ilgi grupları belirlenir ve ilgili personel tarafından takip edilir. USOM tarafından yayımlanan https://www.usom.gov.tr/tehdit.html adresinden yaygın kullanılan yazılım ve donanımlarla ilgili güvenlik bildirimleri takip edilebilir.

3.1.12. Sunuculara yapılan erişimlerin raporlanması, mesai saati dışındaki erişimlerin işaretlenmesi gibi detaylar gözlenir. Kullanıcılara olması gerekenden fazla yetki tanımlanmaz.

3.1.13. Sunuculara ve uygulamalara yapılan başarılı ve başarısız girişimlerin kayıtları tutulur.

3.1.14. Sunucularda oturum açmış kullanıcı hesapları ile herhangi bir işlem yapılmadığı takdirde 10 (on) dakika sonra ekran kilitlenir ve ilgili kullanıcının oturum açma ekranına düşmesi sağlanır. 1 (bir) saat boyunca işlem yapılmadığı takdirde, ilgili kullanıcının oturumu otomatik olarak sonlandırılır.

3.1.15. Bir sunucuda mümkün olduğu kadar az sayıda kullanıcı hesabı bulundurulur ve gereksiz hesap açılmaz. Güvenlik amacıyla başkaca bir zorunluluk yok ise misafir (Guest) hesabı kapalı olarak tutulur. Açılmış fakat kullanılmayan kullanıcı hesapları kapalı duruma (disabled) getirilir veya silinir.

3.1.16. Sunucuların güvenliğini sağlayabilmek için kullanılmayan uygulamalar veya servisler kapatılır. Gerekli servis ve hizmetler dışında başka bir servis çalıştırılmaz.

3.1.17. Sunuculara güvenli bağlantı yapılacak ise SSL sertifikası yüklenir. Sunuculara SSH bağlantısı yapılacak ise kullanılan anahtarlar belirli aralıklarla değiştirilir.

3.1.18. Sertifika kullanım süresi, son kullanım süresi yaklaşan sertifikaların takibi gibi işlemler hazırlanacak bir sertifika takip listesi vasıtasıyla takip edilir.

3.1.19. BIOS güncellemeleri takip edilir. Sunucuların BIOS ayarlarının girişi parola ile korunur. Sunucuların varsayılan olarak CD-ROM, DVD-ROM veya flash disk gibi harici kaynaklardan başlatılması engellenir.

3.1.20. Sunucuda depolanan veriler, işletim sisteminin çalıştığı disk bölümünden farklı bir disk bölümünde tutulur.

3.1.21. Sunucuların arka planda çalışan servisleri ile birlikte o servislerinde kullandığı portlar kontrol edilir. Gereksiz portlar kapatılır. Mümkün olduğu surette uygulamaların varsayılan portları değiştirilir.

3.1.22. Güvenlik testleri yapılarak sunucular ve sistem ile ilgili açıklıklar tespit edilir. Tespit edilen açılıkların kapatılması sağlanır. (Sunucuda Windows işletim sistemi kullanıyor ise "Netstat –an", Linux işletim sistemi kullanıyor ise "Netstat –tulp" komutu ile açık veya kullanılan portlar listelenerek kontrol edilebilir.)

3.1.23. Sunucu işletim sistemleri, güvenlik açıklarına karşı güncel tutulur.

3.1.24. Sistem kaynaklarının uygun seviyede planlanması, sürdürülebilmesi ve etkin kullanılabilmesi için kapasite yönetimi yapılır. Kapasite yönetim planları uyarınca sunucuların performans gereklilikleri belirlenir. Sistemde belli aralıklarla disk birleştirmesi (defragment) ve disk temizlemesi yapılır. Yasal bulundurma süresi dolan veya sistem tarafından geçici olarak yaratılan dosyalar silinir. Disklerin doluluğu, ram ve işlemci kullanımı ve bunlara ilişkin kullanım parametreleri kontrol edilir.

3.1.25. Sunucuda paylaşıma açılmış klasörlerde izin verilen kullanıcı ve gruplar kontrol edilir. Kullanıcılara, gruplara verilen izinler ve kullanıcıların baskın izin seçeneğini nerden aldığı incelenir. Herkes (everyone) isimli kullanıcı grubuna izin atanmaz. İzinler kullanıcılardan ziyade gruplara verilir. Kullanıcıların bilgisayarlarını günlük işlerini yapmalarını sağlayacak seviyede en az yetki ile çalıştırmaları sağlanır. Aynı izinlere sahip olması gereken kullanıcılar bir grupta toplanır.

3.1.26. Sunucularda yapılan işlemlerin iz kayıtlarına erişmek için olay günlükleri (event logs) tutulur.

3.1.27. Sunucu ve sistem güvenliğini sağlayabilmek için lisanslı yazılımlar kullanılır. Kurumun yazılım lisans varlıklarının sayısı, bu lisanların hangilerinin aktif kullanıldığı, kullanılmayan lisansların bilgisinin tutulması gibi ayrıntıları içeren listeleme ile aktif lisans yönetimi yapılır.

3.1.28. Sunucuların fiziksel güvenliğini sağlamaya yönelik tedbirler alınır. Sunucu odası dışında sunucu bulundurulmaz. Sunucu/sistem odalarına yapılan giriş çıkışlar kontrol edilir, giriş çıkış kayıtları tutulur.

3.1.29. Sunucuların üretici tarafından tavsiye edilen/teknik dokümanlarında belirtilen süreler dikkate alınarak yıllık bakım planları hazırlanır. Bakımlar yetkili uzmanlar tarafından yapılır ve kayıt altına alınır.

3.1.30. Sunucuların erişilebilirlik seviyesini artırmak için herhangi bir sunucunun çalışmaması durumun da diğer bir sunucunun onun yerine amaçlanan şekilde çalışmasını sağlayacak kümelenmiş mimari yapıda yapılandırılması gerekir.

4. BGYS Kayıtları

--

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
KURUMSAL KALİTE GELİŞTİRME VE AKREDİTASYON KOORDİNATÖRLÜĞÜ	KURUMSAL KALİTE GELİŞTİRME VE AKREDİTASYON KOORDİNATÖRLÜĞÜ	KURUMSAL YETKİLİ