1. **AMAÇ – KAPSAM :** Üniversitemiz Bilgi İşlem Daire Başkanlığı sunucularına uzaktan yapılan erişimlerde yetkisiz kullanımından dolayı, kritik sistemlere meydana gelebilecek zararları, hassas bilgilerin kaybı ve prestij kaybı önlemek amacıyla sunuculara uzaktan erişime ilişkin standartları tanımlamaktır.

2. **SORUMLULAR :** Bu prosedürün oluşturulmasından ve uygulanmasından Sistem, İdari ve Mali Hizmetler Birimi ile Ağ ve Teknik Servis Alt Yapı Hizmetleri Birimi birlikte 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'ler ile erişim sağlanır. Yerel ağdan bağlanan kullanıcılar yetkili kullanıcı adı ve şifresiyle erişim sağlar.

3.1.2. Üniversitemiz sunucularına uzaktan kimlerin hangi rollerde eriştiğini belirtecek ve ayrıca ilgili kişilerin sunuculara erişimde kullandığı kullanıcı adı ve şifreleri, ilgili birimde gizli olarak tutulacaktır.

3.1.3. Uzaktan erişim trafiği sıkı bir şekilde kontrol edilmelidir. Güvenlik kontrolü tek yönlü şifreleme (one-time password authentication, örnek; token device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmektedir. Daha fazla bilgi için Şifreleme Politikası'na bakınız.

3.1.4. Başkanlık personelimiz, Başkanlığımıza ait hiçbir bilgiyi (idari, mali vb.) kurum dışına çıkartamaz. Aksi taktirde oluşacak yasal yükümlülüklerden kurum sorumlu olacaktır.

3.1.5. Kurum çalışanları hiçbir 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 sahipleri 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. VPN kullanıcıları hat kullanılmadığı takdir de kurumun ağından 30 dakika sonra otomatik olarak bağlantıları kesilmelidir. Kullanıcı tekrar bağlanmak için logon olmak zorunda olmalıdır. Ping veya diğer prosesler network bağlantısını açık tutmak için kullanılmamalıdır.

3.1.8. Uzaktan erişim yöntemi ile kuruma erişen bütün bilgisayarlar en son güncellenmiş anti-virus yazılımına sahip olmalıdırlar.

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

3.1.10. Uzak Masaüstü ile bağlantı yapılacak olan kullanıcılar, Bilgi işlem Daire Başkanlığı envanterinde bulunan cihazlar ile bağlanmak zorundadırlar. Ancak "iş sürekliliğinin sağlanması, işletilmekte olan sunucu ve sistemlere uzaktan destek verilmesi" gibi çok acil hallerde, başka bir imkân olmadığı için şahsi bilgisayarların kullanılması durumunda, kurumsal verilerin söz konusu bilgisayara indirilmemesi ve işlenmemesi için gerekli özen gösterilir. Yapılan müdahalenin doğası gereği bilgisayara indirilen verilerin güvenli olarak silinmesi, işlemi gerçekleştiren kişilerin sorumluluğundadır.

3.1.11. Üniversitemiz web tabanlı e-posta sistemi, EBYS,kurumsal portal gibi doğrudan uygulama erişimleri de dâhil olmak üzere uzaktan çalışmanın hiçbir çeşidinde, sahibi bilinmeyen/herkes tarafından erişilebilen internet kafe, otel bilgisayarları, kiosk vb. ortamlar kullanılamaz.
3.1.12. Uzak Bağlantı işleminden önce Cihazlara kişisel güvenlik duvarı kurulur ve aktif hale getirilir.
3.1.13. İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması sağlanır.
3.1.14. Uzaktan bağlantı için kullanılacak Cihaz üzerinde uzaktan çalışma için kullanılmak üzere asgari yetkilere sahip ayrı bir kullanıcı hesabı açılır. Yönetici yetkisi ile uzaktan çalışma yapılmaz.
3.1.15. Uzaktan bağlantı için kullanılacak Cihaza ekran koruma süresi konularak belli bir süre kullanılmadığında ekranın otomatik olarak kilitlenmesi sağlanır.
3.1.16. Uzaktan bağlantı için kullanılacak Cihazlar fiziki güvenliği olmayan ortamlarda kullanılacak ise "dizüstü bilgisayar kilidi ve güvenlik kablosu" kullanılmak suretiyle çalınmaya karşı cihaz emniyete alınır.
3.1.17. Cihazın üzerinde yer alan ve kullanılmayan ağ özellikleri (Wi-Fi, Bluetooth vb.) pasif hale getirilir.
3.1.18. Disk şifreleme vb. araçlarla bilgisayarlarda tutulan verilerin şifreli olarak saklanması sağlanır.
3.1.19. Uzaktan çalışma için kullanılan bilgisayarların yerel disklerinde yer alan kurumsal verilerin yedeklenmesi için gerekli tedbirler alınır. Alınacak bu yedekler sadece şifreli ortamlarda ve/veya şifreli yedeklenmiş olarak tutulabilir.
3.1.20. Uzaktan çalışma ve uzaktan erişim için kullanılacak cihazlara çok faktörlü kimlik doğrulama yapılarak giriş yapılması tercih edilir.
3.1.21. Uzaktan bağlantı yapacak tüm dış paydaşlarla gizlilik sözleşmesi imzalanması zorunludur.

4. BGYS Kayıtları

- **PR.08-FR.01 VARLIK ENVANTERİ**

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