1. AMAÇ

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesine ait internet ağının ve sunucu sistemlerinin güvenliğinin sağlanabilmesi için uygulanacak kuralları oluşturmayı amaçlar.

2. KAPSAM

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesinin ait tüm ağ ve sistemleri kapsamaktadır.

3. SORUMLULAR

- Bilişim Sistemi Kullanıcıları
- Bilgi İşlem Daire Başkanlığı
- Sistem Yönetimi Birimi

4. TANIMLAR

Firewall: Güvenlik duvarı, güvenlik duvarı yazılımı
BGYS: Bilgi Güvenliği Yönetim Sistemi
Router: Yönlendirici
Switch: Dağıtıcı

5. UYGULAMA

Ağ Güvenliği

Üniversite ağı sadece iş amaçlı kullanılır. Üniversite ağı üzerindeki bilginin korunması yönetimin sorumluluğundadır. Üniversite bilgisayar ağları üzerinde gerçekleştirilen faaliyetler ve bilgilerin içeriği yönetimin gerçekleştirdiği gözden geçirmenin kapsamındadır. Üniversite ağ güvenlik sistemleri ve prosedürleri geliştirip uygular ve tüm kamu verisini, ilgili uygulama sistemlerini ve işletim sistemi yazılımlarını yetkisiz ve yasadışı erişimlere karşı korumak için uygun ağ güvenlik kaynaklarını (Firewall, IDS vs.) sağlar.

5.1 Ağ Erişim Yönetimi

5.1.1 Ağ Hizmeti – İş Tanımı Matrisi

Ağ yöneticileri, Bilgi Güvenliği Yöneticisi'nin yardımıyla Üniversite'de kullanılan tüm ağ hizmetlerini (E-posta, Internet, Telnet, SSL-VPN, Ağ dosya sunucusu, FTP vs.) tanımlarlar. Ağ yöneticileri ayrıca ağ hizmetleri üzerindeki yetkilendirmeyi yönetmekle yükümlüdür. Üniversite bünyesinde sağlanan bu ağ hizmetlerinin hangi birimlere ve görev tanımlarına göre tesis edileceği, Bilgi Güvenliği Yöneticisi ve Bilgi İşlem Yöneticisinin onaylayacağı bir "Ağ Hizmetleri – Personel Görevleri" matrisi ile dokümante edilir.Örneğin e-posta hizmetleri istinasız bütün personele sağlanabilirken, FTP sunucularına erişmek ve

dosya aktarma yetkisi sadece kısıtlı birimde bulunabilir. Bu çalışma sonunda, erişim hakları ile beraber tüm ağ hizmetleri tanımlanmış ve dokümante edilmiş olur. Bu tanımlar, Bilgi Güvenliği Yöneticisi tarafından gözden geçirilir ve Bilgi İşlem Yöneticisi tarafından onaylanır. Bu çalışma ağ hizmetleri ilk defa uygulamaya alınacağı zaman yapılır.Ağ Hizmeti Personel Görevleri Matrisi, yeni bir iş fonksiyonu yaratıldığında veya ağ hizmetleri ciddi ölçüde değiştirildiğinde ağ yöneticileri tarafından değiştirilir. Ağ Hizmeti – Personel Görevleri Matrisi'nde yapılan değişiklik, uygulamaya alınmadan önce Bilgi Güvenliği Yöneticisi tarafından kontrol edilir ve Bilgi İşlem Yöneticisi tarafından onaylanır. Bilgi Güvenliği Yöneticisi Ağ Hizmeti – Personel Görevleri Matrisi'nin hazırlanmasından ve güncel olarak saklanmasından sorumludur.

5.1.2 Ağ Erişiminin Açılması

Bkz. "Erişim Kontrolü Prosedürleri" bölümündeki 'Yeni Kullanıcı Hesabı Açma Talebi'. Üniversite bünyesinde görev tanımı gereği özel olarak yasaklanmadıkça bütün personelin Internet ve e-posta hizmetlerine erişimi vardır. Bu hizmetlere yönelik onay süreci bu prosedürün onaylanmasını takiben gerçekleştirilmiş olarak varsayılır.

5.1.3 Ağ Erişim Haklarının Gözden Geçirilmesi

Bkz. "Erişim Kontrolü Prosedürleri bölümündeki " '*Erişim Haklarının Gözden Geçirilmesi'*.

5.1.4 Üçüncü Parti Erişimi

Üniversitenin, öğrenci, misafir, hizmet sağlayıcı gibi üçüncü taraflara ağ erişimi sağlaması gerekebilir. Üniversite diğer taraflar ile elektronik işlemlerini yapabilmeleri veya bilgi paylaşımında bulunabilmeleri amacıyla başka kuruluşlara ağ üzerinde standart ya da yüksek yetkili erişim hakkı tanıyabilir. Bu gibi durumlarda, diğer taraflarla ilişkilerin yönetilmesinde aşağıdaki prosedürler izlenir:

İş süreci sahipleri üçüncü taraflara erişim açılması için işlemleri Yardım Masası üzerinden başlatır. Uzun süreli (bir günden daha uzun) erişim ihtiyacı için, Üniversite, sağlanan erişim için üçüncü partiyle önce bir anlaşma / sözleşme imzalar. Bu anlaşma / sözleşme aşağıdakileri içerir:

- Paylaşılacak bilgi
- Erişecek kişiler
- Erişimin gerekli olduğu işlemler
- Gerekli olan erişim seviyesi
- Bilgi paylaşımı / gerçekleştirilecek işlem için gerekli güvenlik mekanizmaları

- Üçüncü parti üzerinde uygulanabilecek güvenlik politikalarının detayları
- Üniversite amacı dışında kullanılmasına yönelik yasal yaptırımlar

Üçüncü taraflar Ağ Erişimi için Yardım Destek kayıt açar ya da e-posta yoluyla Bilgi İşlem yöneticisinden onay alır. Çağrı ya da e-posta, ihtiyaç duyulan erişim tipi, hangi uygulamanın kullanılacağı, hangi verinin iletileceği, gerekli/kullanılan şifreleme yöntemi vb. konuları içerir. Bu belgeler, sonrasında iş süreci sahibi tarafından üçüncü partiyle iletişime geçilerek onaylanır. Erişim, Bilgi Güvenliği Yöneticisi'nin onayından sonra ağ yöneticisi tarafından sağlanır. Bilgi Güvenliği Yöneticisi, verilecek erişimin güvenlik yapısına etkisini analiz eder. Eğer bir üçüncü partinin, Üniversite kaynaklarına bir günden kısa bir süre için erişim ihtiyacı varsa, üçüncü partiye erişim sağlanırken bir erişim yetki formu veya e-posta onayı hazırlanır ve bu tüm erişim seviyeleri için (read / write) Bilgi İşlem yöneticisi tarafından onaylanır. Üçüncü parti, veri üzerinde değişiklik yapmak istediğinde önce ilgili iş süreci sahibinden onay alır ve bu onayı Bilgi İşlem yöneticisine iletir. Bilgi İşlem Yöneticisi'nden gelen bilgi üzerine ağ yöneticisi, üçüncü parti kullanımı için ayrı kullanıcılar yaratır. Gerekli durumlarda, ağ yöneticileri, üçüncü parti işlemlerini izlemek için işletim sistemi seviyesinde yaratılan denetim izlerini gözden geçirir. Ağ yöneticilerinin amiri ya da ağ yöneticisi (bir amirin olmaması durumunda), bu tip tüm üniversite dışı erişimlerin kaydını tutar ve bu hesaplar üzerinden yapılan bağlantıları düzenli olarak izler. Ayrıca, 2 ayda bir, iş süreci sahipleriyle birlikte, erişimin geçerlilik süresinin bitmesi durumunda, bu hesapların halen aktif olup olmadığını kontrol eder. Eğer bu hesaplar kullanılmıyorsa, o zaman ağ yöneticisi bunun doğruluğunu kontrol eder ve derhal bu erişimleri iş süreci sahibinden yetki alarak iptal eder. Üniversitenin başka kurumların sistemlerine erişimi gerekiyorsa, bu durumda kurum bu kurumların prosedürlerini uygular. Bu konuda diğer kurumların uygulanmasını istediği esaslar, iş süreci sahipleri ve Bilgi Güvenliği Yöneticisi tarafından onaylanır. Bilgi İşlem yöneticisi, bu erişimlerin bir kaydını tutar ve bunları düzenli olarak izler.

5.1.5 İnternet Hizmetine Erişim Talebi

Domain kullanıcılarının yaratılmasının ardından tüm çalışanlara kendi yaptıkları işin kapsamına ve niteliğine göre internet erişimi sağlanır. İnternet erişimine üniversite ağı üzerinden ihtiyacı olan her üçüncü parti çalışanı için, üçüncü taraflarla koordinasyonu sağlayan üniversite çalışanı, erişim talebinin nedenleri ve erişilmek istenen olası sitelerin listesi ile birlikte Bilgi İşlem yöneticisinden e-posta yoluyla talepte bulunur. Ancak üçüncü parti tarafından Internet erişimi, ana ağdan ayrı tutulan misafir ağı üzerinden gerçekleştirilecekse, bu ağın dizaynı ve erişim yetkileri önceden onaylanmış varsayılıp ayrıca onay talep edilmeyecektir. Üçüncü parti tarafından gerçekleştirilen bütün Internet bağlantıları, diğer bütün bağlantılarda olduğu gibi 5651 numaralı "*İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*" uyarınca izlenir. Bu talep, sonrasında Bilgi İşlem yöneticisi tarafından onaylanır ve yetki için Bilgi Güvenliği Yöneticisi'ne iletilir. Onay ve yetki alındıktan sonra sistem ve ağ yöneticisi İnternet erişimini sağlar. Çalışanların domain kullanıcılarının iptal edilmesiyle internet erişimleri otomatik olarak iptal edilir. Üçüncü parti çalışanları ile koordinasyonu sağlayan Üniversite çalışanı, üçüncü parti çalışanlarının Internet erişimi gereksinimi sona erdiğinde

erişimin iptali için ilgili sorumlu Bilgi İşlem Birimine talepte bulunmalıdır. Internet erişimi sağlanmadan önce tüm çalışanların kabul edilebilir kullanım politikasını (bkz. Kabul Edilebilir Kullanım Politikası) okumaları istenmelidir. Internet erişim politikalarını ezen her politika/faaliyet, gerekçeleri sunulduktan sonra, Bilgi İşlem Yöneticisi ve Bilgi Güvenliği Yöneticisi tarafından onaylanacaktır. Örneğin, erişimin yasaklandığı sitelere erişim veya bir yazılımın bilgisayara indirilmesi olabilir.

5.1.6 Herkese Açık Alanlarda Ağ Erişiminin Kısıtlanması

Herkese açık alanlarda ve toplantı odalarındaki ağ bağlantı noktalarından Üniversite ağına erişim kısıtlanır. Bu ağ bağlantılarının kullanımı Bilgi İşlem yöneticisi tarafından onaylanır.

5.1.7 Erişim Yetkilerinin Periyodik Olarak Doğrulanması

Çeşitli sistemlerin yöneticileri periyodik olarak tüm kullanıcı hesaplarının geçerliliğini, ilgili bölüm yöneticileri birlikte tekrar doğrular. Doğrulama periyodu altı aydan uzun olamaz.

5.1.8 İnternet Hizmetinin İzlenmesi ve Denetim İzinin Tutulması

Gerektiği takdirde hangi web sitelerinin hangi kullanıcı tarafından ziyaret edildiği, hangi dosyaların indirildiğine dair denetim izleri Bilgi İşlem ekibi tarafından gözden geçirilir. Bilgi İşlem ekibi, olağandışı olayları Bilgi İşlem yöneticisi ve Bilgi Güvenliği Yöneticisi'ne raporlar. Kimlik doğrulama için kullanılan kullanıcı veritabanı olağandışı faaliyetleri tespit etmek amaçlı her hafta gözden geçirilir. Olağandışı faaliyet:

- Bir kullanıcının hesabına 5'ten fazla başarısız giriş denemesi
- Yüksek yetkili kullanıcı hesaplarına erişim denemesi

Bu gibi aktivitelere ait raporları Bilgi İşlem yöneticisi ve Bilgi Güvenliği Yöneticisi gözden geçirir ve bunları, kendi birimlerinin işletme faaliyetleri için uygun olan internet erişim tipini belirlemek için kullanır.

Elektronik yazışmalar üzerinden gelen tüm güvenlik bildirimi mesajları öncelikle Bilgi Güvenliği Yöneticisi veya Bilgi İşlem Yöneticisi'ne gelir ve buradan dağıtılır. Eğer herhangi bir kullanıcı diğer bir dış kaynaktan bu gibi bir güvenlik bildirimi mesajı alırsa, bu durumu Bilgi Güvenliği Yöneticisi veya Bilgi İşlem Yöneticisi'ne bildirir ve mesajı bu kişiler dışında kimseye dağıtamaz.

Kuruluşun internet erişimini sürdürme sorumluluğu Bilgi İşlem ekibindedir. Bu ekip, yeni güvenlik açıklıklarından veya tehditlerinden haberdar olmak için Üniversitenin üyesi olduğu internet güvenliği haber gruplarını ve diğer uygun forumları takip eder ve kuruluşun internet bağlantısında gerçekleştirilmesi gerekli herhangi bir değişikliği zamanında koordine eder.

5.2 Ağ Yönetimi

5.2.1 Ağ Donanımlarının Tanımlanması

Altyapı işleri sorumlusu tüm ağ donanımlarını isimleriyle tanımlar ve bunların, yer ve amaçları ile ağ spesifikasyonlarının bir kaydını tutar. Ağ altyapısının yönetimi için örn: HP Intelligent Management Center aracı kullanılır ve bu araç üzerinde ağ donanımlarının ayarları ilgili Bilgi İşlem sorumlusu tarafından yapılır. Donanım ve ekipmanlar üzerindeki değişiklikler konfigürasyon sorumluları tarafından gerçekleştirilir.

Tüm ağ ve sunucu donanımlarının – yerel ağ sunucuları, köprü (bridge), Router, switch, hub gibi donanımlar da dâhil - fiziksel güvenliği, yetkisiz erişimlere karşı, kilitli ve erişimin kısıtlı olduğu odalar ya da dolaplar kullanılarak sağlanır. Ağ altyapısında kullanılan cihazların genel kullanımındaki fiziksel güvenlik sorumluluğu üniversitededir.

Teknik olarak mümkün olan yerlerde, çok hassas işlemler, bu işlemlerin çalıştırılabileceği terminaller kısıtlanarak güvenlik altına alınır. Bu terminallerin fiziksel (klavye kilitleri vb.) ve/veya mantıksal güvenliği sağlanır.

5.2.2 İletişim Hatlarının Tanımlanması

Entegre iletişim hatları (Ağ hatları, GSM data hatları vb.), bakım ve güvenliğin sürdürülebilmesi için sınıflandırılır ve erişilen sistem için özgün olması sağlanır. Tüm hatlar kapasiteleriyle birlikte dokümante edilir ve Bilgi İşlem ekibi tarafından yönetilir.

Ses ve/veya veri iletimi için kullanılan tüm kablo ve hat donanımlarının güvenliği sağlanır. Eğer hatların güvenliği sağlanamıyorsa, Bilgi İşlem ekibi ve haberleşmeden sorumlu yönetici personel bunun nedenlerini dokümante eder ve Bilgi İşlem Daire Başkanına iletir.

5.2.3 Ağ Değişiklik Yönetimi

Firewall kural değişiklikleri, konfigürasyon değişiklikleri, ağ altyapısındaki gelişmeler gibi ağ bileşenlerinde gerçekleşebilecek herhangi bir değişiklik için Operasyonel Değişiklik Yönetimi Prosedürleri izlenir (Bkz. İletişim ve Operasyon Yönetimi – Operasyon Değişikliği Yönetim Prosedürleri).

5.2.4 Ağ Şeması

Bilgi İşlem yöneticisi ve Altyapı sorumlusu ağ şemasının güncelliğinden sorumludur. Bilgi Güvenliği Yöneticisi ağ şemasını, şemanın mevcut ağ yapısını yansıtacak şekilde güncellendiğini kontrol etmek amacıyla periyodik olarak gözden geçirir. Ağ yapısında bir değişiklik gerçekleştiğinde, ağ şemaları güncellenir.

Ağ şeması aşağıdaki detayları içerir:

Şema Geniş Alan Ağ (WAN) yapısından Yerel Ağ (LAN) parçalarına kadar birçok katman içerir.

1. Katman – Geniş Alan Ağı

2. Katman – Yerel Ağlar

3. Katman – Yerel Ağ Parçaları

Ağ şeması IP adresleriyle beraber tüm ağ donanımlarını gösterir.

Ağ şeması kullanılan protokollerle beraber Geniş Ağ hattının tipini de içerir.

Ağ Şeması tüm iletişim hatlarını (asıl ve yedek hat), bu hatların bant genişliğini ve hat üzerinde iletilen verinin tipini (ses / veri) içerir.

Ağ şemasını yönetmek ve güncellemek için yeterli seviyede versiyon kontrol mekanizmaları kullanılır.

5.3 Asgari Güvenlik Standartları

Bilgi Güvenliği Yöneticisi tüm ağ donanımları için (Router, Firewall, Modem vs.) Asgari Güvenlik Standartları (AGS) oluşturulmasını sağlar. Bilgi Güvenliği Yöneticisi aynı zamanda tüm ağ donanımlarının AGS' ye göre yapılandırılmasını sağlar. Tüm ağ elemanları herhangi bir kullanıcı giriş yaptığında aşağıdaki mesajı vermek üzere yapılandırılır:

"Bu sistem sadece yönetim onaylı işlemlerin yapılması için yetkili kullanıcıların kullanımı içindir. Bu sistemlere yetkisiz erişim yapılması veya kişisel amaçlı kullanımı yasaktır. Yetkisiz olarak erişen kişiler haklarında yürütülecek hukuki ve/veya disiplin soruşturmalarına tabi olacaklardır. Bu erişim esnasında herhangi bir kanun ya da yönetmelik dışı hareket gözlemlendiğinde bu denetim izleri kanuni delil olarak kullanılabilir." En son güvenlik konfigürasyonlarını içermesi için, Bilgi Güvenliği Yöneticisi AGS'yi yılda bir defa gözden geçirir ve gerektiğinde günceller. Bilgi Güvenliği Yöneticisi her bir iş biriminin Bilgi Güvenliği Yöneticisi ile çalışarak tüm firewall, Router gibi ağ donanımı ve ayrıca işletim sistemi, veritabanı ve uygulama kurulumlarını, bu kurulumların AGS'ye göre yapıldığını kontrol etmek için yılda bir defa gözden geçirir. Gözden geçirme bulguları Bilgi İşlem yöneticisi ve Güvenlik Kurulu'na sunulur.

5.4 Ağ Bileşenlerinin Yönetimi ve Ağ Trafiğinin Takibi

Ağ ekibi öncelikle ağ yönetiminden sorumludur. Tüm ağ donanımlarının kurulumunda, yapılandırılmasında ve bakımında görev alır. Üniversite bünyesinde genel olarak ağların yönetimi ve trafiğin takibi Sistem ve Network Uzmanı'nın sorumluluğundadır. Ancak Üniversite, Sistem ve Network Uzmanı'nın bu yönetim ve takip görevlerini, bu prosedürde yazan prensiplere ve kurallara uygun olarak gerçekleştirdiğinin takibinden sorumludur. Ağ ekibi, ağ donanımlarının kurulumu için tedarikçinin sağladığı kılavuzları kullanır. Ağ ekibi tüm ağ donanımlarını Bilgi Güvenliği Yöneticisi'nin oluşturduğu AGS'ye göre yapılandırır. Ağ trafiğinin gerçek zamanlı izlenmesi ve sorunların çözülmesi Üniversitenin belirlediği üçüncü partiler tarafından tanımlanan SLA'ler çerçevesinde

gerçekleştirilir. Ağ üzerindeki işlemler, aşağıda listelenen olağandışı durumların zamanında tespit edilmesi ve gerekli iyileştirici faaliyetlerin zamanında gerçekleştirilmesi için sürekli izlenir. Router/Firewall/IDS konfigürasyon tablolarındaki (Ağ trafiği üzerinde Router'da gerçekleştirilen adres filtrelemesi gibi) değişiklikler Şifre değişikliklerinin ağ izleme sisteminde alarm üretilmesi gibi Router/Firewall/IDS konfigürasyon ve erişiminde gerçekleşen değişiklikler Router/Firewall/IDS' teki erişim kaybının, problemin çözümü için denetim izinin Ağ bileşenlerinin denetim izleri haftada bir defa ve bir olayla karşılaşıldığı durumlarda gözden geçirilir. Ağ donanımlarında karşılaşılan ve herhangi bir iş sürecinin gecikmesine veya durmasına sebep olacak tüm problemler "Olay" olarak sınıflandırılıp, Olay Yönetimi Prosedürü'nde belirtildiği şekilde ele alınır ve yönetilir.

5.5 Veri İletimi

5.5.1 Şifreleme Teknolojisinin Kullanımı

Bkz. Şifreleme Sistemleri

5.6 Ağ Değerlendirmesi

Üniversite ağında bulunan tüm bilgi kaynakları üzerinde, bilinen yazılım hatalarının ve zayıflıklarının tespiti için sürekli olarak zafiyet değerlendirmesi gerçekleştirilir. Bu faaliyet Bilgi Güvenliği Yöneticisi tarafından koordine edilir. Oluşan güvenlik açıkları devamlı olarak takip edilir ve sistemler test edilir. Bilinen tüm yazılım hatalarına karşı yeterli sayıda test yapılır. Değerlendirme sırasında zafiyetler belirlendikçe, uygun aksiyonlar alınır. Bilgi Güvenliği Yöneticisi ve Bilgi İşlem Ekibinin diğer çalışanları değerlendirmenin yapılacağı varlıkların listesini hazırlar. Tüm varlıklar için belirlenen aralıklarla varlık değerlendirme çalışması yapılır. Bilgi İşlem yöneticisi tüm ağ kaynaklarının AGS'ye göre yapılandırıldığını doğrular. Değerlendirmenin yapılması için güvenilirliği kanıtlanmış Zayıflık Değerlendirme ve Yönetim araçlarının kullanılmasını sağlar. Bilgi İşlem ekibi tarafından kullanılan zayıflık değerlendirme ve yönetim araçlarının sonuçları her ay Bilgi İşlem yöneticisine detaylı bir değerlendirme raporu olarak sunulur. Bu raporlardan oluşturulan özet rapor ise Güvenlik Kurulu'na sunulur. Yönetime, öğrencilere, misafirlere ve Üniversite ağına dâhil olan diğer taraflara güvence sağlamak amacıyla her yıl bağımsız bir üçüncü partiye ağ güvenliği değerlendirme testi yaptırılır. Bu testin sonucunda tespit edilen bulgular Bilgi Güvenliği Yöneticisi tarafından değerlendirilir ve Güvenlik Kurulu'na bir yönetim özeti raporu olarak sunulur.

5.7 Uzaktan Erişim Güvenliği

Dial-Up/Uzaktan Erişim Onayı ve Kaydı – kuruluş çalışanları veya üçüncü tarafların kullandığı dial-up veya uzaktan erişim ile ilgili hizmet ya da bileşene sahip olan ve yeni alınan sistemler veya hizmet talepleri Bilgi İşlem yöneticisi tarafından gözden geçirilir ve onaylanır. Gözden geçirme ve onay süreci aşağıdaki hususlara göre değerlendirilir:

- Talep edilen dial-up/uzaktan erişim uygulamasının uygunluğu
- Erişim noktaların giriş noktalarının seçim kriterlerinin uygunluğu

- Eğer geniş bant bağlantı hizmeti mevcut değilse, onaylanmış bir internet hizmet sağlayıcı kullanılması
- Dial-up/uzaktan erişen kullanıcıların kimlik doğrulamasında kabul edilebilir risk ve maliyet seviyelerin belirlenmesi
- Erişimin onaylanması için bir uzaktan erişim talebi
- İlgili hizmetin, yazılımın veya donanımın izlenmesi

Uzak erişim bilgileri – Çevrimiçi uygulamalara erişmek için kullanılan bilgiler iş ihtiyacı dışında paylaşılamaz. Bilgi İşlem yöneticisi uzaktan erişen kullanıcıların bir listesinin oluşturulmasını sağlar. Bu liste uzaktan erişimi sağlayan sistem üzerinde elektronik olarak da tutulabilir.

Yerel Ağlara/Sistemlere Doğrudan Uzaktan Erişim – Yerel ağ ve sistemlere doğrudan uzaktan erişim onaya tabidir. Bilgi İşlem bölümü tarafından daha önceden onaylanmış olan uzaktan erişimlerin, donanım, kullanılan iletişim yazılımı ve ulaşılan yazılımı içeren bir listesi tutulur.

İş İstasyonlarına Uzaktan Erişim – İş istasyonlarına doğrudan uzaktan erişim onaya tabidir. Bilgi İşlem bölümü iş istasyonlarına uzaktan erişim yetkisi onaylanmış kullanıcıların ve eriştikleri iş istasyonlarının bir listesini tutar.

Tespit/Bakım Bağlantı Noktalarına (Port) Uzaktan Erişim – Tüm uzaktan tespit/bakım (diagnostics) bağlantı noktaları erişime kapatılır. Gerektiği durumlarda yalnızca yetkili kullanıcılara tespit/bakım bağlantı noktalarına ve ilgili donanıma erişim verilir. Güvenli olmayan cihazlar üzerinden uzaktan erişime izin verilmez.

Uzaktan Kontrol Erişimi– Bilgi sistemlerine uzaktan kontrol erişimi için yalnızca Üniversitenin onayladığı uzaktan kontrol konfigürasyonu ve yazılımı kullanılır. VPN ve/veya Anahtar (Token) Üniversitenin ağlarına uzaktan erişim için tercih edilen yöntemlerdir. Kullanımdayken ya da kullanım için beklemedeyken dışarıdan zarar görmelerini engellemek için, uzaktan kontrol edilen tüm işlemcilerin fiziksel güvenliği sağlanır.

Kimlik Doğrulama Yöntemleri – Uzaktan erişim kontrolleri, yalnızca aşağıdaki gerekliliklerin tümünü karşılayan donanım ve yazılım güvenlik araçlarının onaylanmış kombinasyonu ile uygulanır:

- Her kullanıcı için özgün kimlik veya erişim kodu (User ID)
- Kullanıcı erişimini sadece yetki verilen ağ, bilgisayar sistemleri ve uygulamalarla sınırlama kabiliyeti
- Saklanan veri ve güvenlik sisteminin kurcalanmaya karşı koruyan erişim kontrolü yazılımı/donanımı
- Başarılı ve başarısız giriş denemelerinin denetim izleri
- Başarısız giriş denemelerinin sayısını kısıtlama kabiliyeti

6. İLGİLİ DOKÜMAN

- Ağ Güvenliği Politikası
- Erişim Kontrolü Prosedürü
- Şifreleme Sistemleri Prosedürü

	Ağ Güvenliği Prosedürü	Doküman No	PR.09
		İlk Yayın Tarihi	20.02.2018
		Revizyon No	0
		Revizyon Tarihi	
		Sayfa No	

Hazırlayan		Onaylayan