

Üniversitemizin iç taleplerine zamanında ve doğru çözümler bulabilmemiz için yasal mevzuata uygun şekilde verinin bütünlüğünün sağlanması için:

- Oryantasyon aşamasında personele gerekli bilgiler aktarılmış,
- Gereklı altyapı ve donanım belirlenmiş,
- Gereklı altyapı ve donanımın kesintisiz olarak sağlanması için, gereklı kaynaklar ayrılmış,
- Üniversitemizin, akademik ve idari personeller, öğrenciler ve üniversitemize gelen misafirlerimizin, hastanemizde tedavi olan hastalarımızın bilgilerinin korunması açısından yapılması gerekenler personelimize eğitimlerle aktarılmış, üniversite çalışanlarımıza “iş sözleşmeleri” ile sorumlulukları yazılı hale getirilmiş,
- Tüm verilerin yedeklenmesi amacıyla gereklı alt yapı belirlenip, sorumlular tanımlanmış,
- Network üzerinde gereklı erişim işlemleri sınırlandırılmış,
- Bilgi güvenliği konusundaki 3 temel prensibi gizlilik, bütünlük ve yetkililerce erişilebilirlik prensipleri belirlenmiştir.
- Üniversite politikaları doğrultusunda içerik filtreleme sistemleri kullanılmıştır. İstenilmeyen siteler (zararlı yazılım, oyun, kumar, şiddet içeren vs.) yasaklanmıştır.
- Üniversite ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmaktadır.
- Üniversite ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılmaktadır, internete giden ve gelen bütün trafik virüslere karşı taranmaktadır.
- Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri belirlenmiştir.
- Ancak yetkilendirilmiş kişiler internete çıkarken, normal kullanıcılarının bulunduğu ağdan farklı bir ağda olmak kaydıyla, bütün servisleri kullanma hakkına sahiptir.
- Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemelidir.
- İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilmemeli ve indirilmemelidir. Bu konuda gereklı önlemler alınmalıdır.
- Üçüncü şahısların internet erişimleri için misafir ağı erişimi verilmektedir.

- 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) gereği kurum internet erişim kayıtları en az iki yıl arşivlenmektedir.
- Tunnel platformları, VPN (Kurum Dışı VPN), PROXY ve DNS değişiklikleri yapılarak internete bağlanması yasaktır.
- ICQ, GTALK, SKYP vb. mesajlaşma yazılımları kullanılamaz.
- Başkalarının fikri haklarını ihlal edici (copyright) materyalin (yazı, makale, kitap, film, müzik eserleri vb.) dağıtımı yasaktır.
- Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Kurum bu tür ihlallerin söz konusu olduğu durumları inceler ve bir suç olduğundan şüphe duyulursa Disiplin Prosedürüne göre karar alınır veya yasa uygulayıcısı ile işbirliği yapabilir.
- Kurum hesaplarına ait kullanıcı adı ve şifrenizin internet üzerinden paylaşılması yasaktır.
- Kurum içerisinde kullanılan kullanıcı adı ve şifreler ile sosyal hayatta kullanılan kullanıcı adı ve şifrelerinin aynı olması yasaktır.
- Kurum network ağına kurum dışı cihazların takılması yasaktır.