(Tekirdağ Namık Kemal Üniversitesi Senatosunun 16/06/2016-06 tarih ve 28 sayılı kararı) **YÖNERGE**

TEKİRDAĞ NAMIK KEMAL ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI VE BİLGİ GÜVENLİĞİ YÖNERGESİ

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç
Madde 1- (1) Bu yönergenin amacı; Tekirdağ Namık Kemal Üniversitesi'nin görevi ve konumu nedeniyle bilgi çağı gereklerine paralel olarak bilgi paylaşımı ve güvenliği konularında tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek, içeriden ve/veya dışarıdan gelebilecek kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak ve yürütülen faaliyetleri etkin, doğru, hızlı ve güvenli olarak gerçekleştirmektir.

Kapsam
Madde 2- (1) Bu yönerge, Tekirdağ Namık Kemal Üniversitesine bağlı akademik ve idari teşkilatında bulunan bütün birimlerdeki personelin, bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

Hukuki Dayanak
Madde 3- (1) Bu Yönerge, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna dayanılarak hazırlanmıştır.

Tanımlar
Madde 4- (1) Bu yönergede geçen;
Rektör: Namık Kemal Üniversitesine Rektörünü,
Üniversite: Namık Kemal Üniversitesini,
Daire Başkanlığı: Bilgi İşlem Dairesi Başkanlığını,
Sistem Yöneticisi: Sorumluluk Kabul Formu(EK-5) ile bilgi işlem daire başkanlığı bünyesinde görevlendirilmiş yetkin Bilgi Sistemleri Yöneticisini,
Kullanıcı: Üniversite Bilgi Sistemlerini Kullanan tüm kişileri,
Sunucu: İstemcilerden gelen isteklere hizmet verebilen bilgisayar sistemini,
İstemci: Sunucuların verdiği hizmeti alan bilgisayar sistemini,
İfade eder.

(2) Yönergede kullanılan teknik terim ve tanımlar,
Zincir e-posta: Bir kullanıcıya gelen şans ve para kazanma yöntemleri gibi bir içeriğe sahip e-postanın art arda diğer kullanıcılara gönderilmesi,
Spam: Yetkisiz ve/veya istenmeyen reklam içerikli e-postalar,
Sahte e-posta: Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenini kazanmak ve kişisel bilgilerine (tamamen yasadışı yoldan) erişmek,

RADIUS (Remote Authentication Dialin User Service): Sunucular uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan internet protokolü,
X.509/LDAP(Light weight Directory Access Protocol): Aktif dizin ve e-posta gibi programlardan bilgi aramak için kullanılan bir internet protokolü,
Portal: Birden çok içeriği bir arada bulunduran alan,
SSL (Secure Socket Layer): Ağ üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş bir güvenlik protokolü,
VPN: Bir ağa güvenli bir şekilde, uzaktan erişimi sağlayan teknoloji
IPSec (Internet Protocol Security)VPN: Genel ve özel ağlarda şifreleme ve filtreleme hizmetlerinin bir arada bulunduğu ve bilgilerin güvenliğini sağlayan iletişim kuralı ile uç kullanıcıya güvenli uzaktan erişim sağlama,
IP: Bilgisayar ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alış verişi yapmak için kullandıkları adres,
MAC adresi: Bir ağ cihazının tanınmasını sağlayan kendisine özel adres,
SNMP: Bilgisayar ağları üzerindeki birimleri denetlemek amacıyla tasarlanmış protokol,
Firmware: Sayısal veri işleme yeteneği bulunan her türlü donanımın kendisinden beklenen işlevleri yerine getirilebilmesi için kullandığı yazılımlar,
DMZ: Üniversite içi ağı ile Üniversite dışı ağı birbirinden ayıran bölge,
Uzaktan Erişim: İnternet, telefon hatları veya kiralık hatlar vasıtası ile Üniversitenin ağına erişilmesi,
Risk: Üniversitenin bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörler,
Güvenli Kanal: Güçlü bir şifrelemeden oluşan iletişim kanalı,
Uygulama Sunucusu: Dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımıdır. Üç katmanlı uygulamaların bir parçasıdır.
Bu üç katman: Kullanıcı arayüzü (GUI), uygulama sunucusu ve veritabanı sunucusu,
Yetkilendirme: Sisteme giriş izni verilmesi, çok kullanıcılı sistemlerde sistem yöneticisi tarafından, sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği işlemler için belirli izinler verilmesi,
Yedekleme: Ekipmanın bozulması durumu düşünülerek dosyaların ve/veya veritabanının başka bir yere kopyalanması işlemi.
Veritabanı: Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğu,
Şifreleme: Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan özel bir algoritma
VLAN (Virtual LAN) Sanal yerel ağ: Birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurmaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubu.

İKİNCİ BÖLÜM
Bilgi Güvenliği

E-Posta
Madde 5- (1) E-Posta ile ilgili yasaklanmış kullanım kuralları aşağıda belirtilmiştir.
a) Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmez.
b) Üniversite ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilir.

c) Kullanıcı, Üniversitenin e-posta sistemini taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları gönderemez. Bu tür özelliklere sahip bir mesaj alındığında ilgili birime haber verilir.
ç) Kullanıcı hesapları, ticari ve kâr amaçlı olarak kullanılmaz. Diğer kullanıcılara bu amaçlar ile e-posta gönderilemez.
d) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, ilgili birime haber verilir.
e) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmaz.
f) Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) gönderemez.
g) Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların yollanmasından sorumludur.
ğ)Kullanıcılar e-mail taleplerini E-mail talep formu (EK-2) doldurarak yaparlar,

(2) E-Posta ile ilgili kişisel kullanım kuralları aşağıda belirtilmiştir.
a) E-posta kişisel amaçlar için kullanılamaz.
b) Kullanıcı, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidir. Bu yüzden parola kullanılmalı ve kullanılan parola en geç 45 günde bir değiştirilmelidir. E-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
c) Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu epostalara herhangi bir işlem yapmaksızın ilgili birime haber vermelidir.
ç) Kullanıcı, kurumsal mesajlarını, Üniversite iş akışının aksamaması için cevaplandırmalıdır.
d) Kullanıcı, kurumsal e-postalarının, Üniversite dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesini ve okunmasını engellemelidir.
e) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar ilgili birime haber verilmelidir.
f) 6 ay süreyle kullanılmamış e-posta adresleri kullanıcıya haber vermeden sunucu güvenliği ve veri depolama alanının boşaltılması için kapatılmalıdır.
g) Kullanıcı parolaları, en az 8 karakterden oluşmalı ve parolalarının içinde; en az 1 tane harf, en az 2 tane rakam ve en az 1 tane özel karakter (@,^,+,$,#,&,/,{,*,-,],=…) içermelidir.
ğ) Kullanıcı, kendilerine ait e-posta parolasının güvenliğinden ve gönderilen epostalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren ilgili birime haber vermelidir.

(3) Kurumsal e-postalar yetkili kişilerce hukuksal açıdan gerekli görülen yerlerde önceden haber vermeksizin denetlenebilir.

(4) Kullanıcı, e-postalarına erişirken, POP3, SMTP, HTTP vb kullanıcı adı ve parolasını açık metin olarak (okunabilir halde) taşıyan protokolleri kullanamaz.

(5) Üniversite, e-postaların Üniversite bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur.

(6) Virüs, solucan, truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslere bulaşmış e-postalar antivirüs yazılımları tarafından analiz edilip, içeriği korunarak virüslerden temizlenmelidir. Ağa dâhil edilmiş bilgisayarlarda ve sunucularda ağ güvenlik yöneticileri bu yazılımdan sorumludur.

Parola

Madde 6- (1) Parola ile ilgili genel kurallar aşağıda belirtilmiştir.
a) Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) en geç 6(altı) ayda bir değiştirilir.
b) Kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) en geç 45(kırk beş) günde bir değiştirilir.
c) Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanır.
ç) Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmez.
d) Kullanıcı, parolasını başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda bilgilendirilir ve eğitilir.
e) Üniversite çalışanı olmayan kişiler için açılan kullanıcı hesapları da kolayca kırılamayacak güçlü bir parolaya sahip olmalıdır.
f) Bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmaz.

(2) Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygular.
a) En az 8 haneli olmalıdır.
b) İçerisinde en az 1 tane harf bulunmalıdır. (a, b, C...)
c) İçerisinde en az 2 tane rakam bulunmalıdır. (1, 2, 3...)
ç) İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,^,+,$,#,&,/,{,*,-,],=,...)
d) Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, ababab...)
e) Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,1234,zxcvb...)
f) Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)

(3) Şifre koruma standartları ile ilgili kurallar aşağıda belirtilmiştir.
a) Bütün parolalar Üniversiteye ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmaz.
b) Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılmaz.
c) Parola kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir.
ç) Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilebilir.

(4) Uygulama Geliştirme Standartları
a) Bireylerin ve grupların kimlik doğrulaması işlemini desteklemelidir.
b) Parolalar metin olarak veya kolay anlaşılabilir formda saklanmamalıdır.
c) Parolalar, şifrelenmiş olarak saklanmalıdır.
ç) En az RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

Antivirus
Madde 7- (1) Antivirus ile ilgili kurallar aşağıda belirtilmiştir.
a) Üniversitenin tüm istemcileri ve sunucuları antivirüs yazılımına sahip olmalıdır. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak antivirüs yazılımı yüklenmeyebilir.
b) İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılır.
c) Sistem yöneticileri, antivirüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
ç) Kullanıcı hiç bir sebepten dolayı antivirüs yazılımını bilgisayarından kaldıramaz.

d) Antivirüs güncellemeleri antivirüs sunucusu ile yapılır. Sunucular internete sürekli bağlı olup, sunucuların veri tabanları otomatik olarak güncellenir. Etki alanına bağlı istemcilerin, otomatik olarak antivirüs sunucusu tarafından antivirüs güncellemeleri yapılır.
e) Etki alanına dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarları ağdan çıkartabilmelidir.
f) Bilinmeyen veya şüpheli kaynaklardan dosya indirilmez.
g) Üniversitenin ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilir.
ğ) Optik Media ve harici veri depolama cihazları antivirüs kontrolünden geçirilir.
h) Kritik veriler ve sistem yapılandırmaları düzenli aralıklar ile yedeklenir ve bu yedekler farklı bir elektronik ortamda güvenli bir şekilde saklanır. Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı olmalıdır.

İnternet Erişim ve Kullanımı
Madde 8- (1) İnternet Erişim ve Kullanımı ile ilgili kurallar aşağıda belirtilmiştir.
a) Üniversitenin bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar(lar)ı üzerinden internete çıkılır. Ağ güvenlik duvarı, Üniversitenin ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında Üniversitenin karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.
b)Üniversitenin uygulamaları doğrultusunda içerik filtreleme sistemleri kullanılır. İstenilmeyen siteler (pornografi, oyun, kumar, şiddet içeren vs.) yasaklanır.
c) Üniversitenin ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılır.
ç) Üniversitenin ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılır. İnternete giden ve gelen bütün trafik virüslere karşı taranır.
d) Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri hayata geçirilir.
e) Ancak İnternet yetkili çıkış formunda(EK-4) yetkilendirilmiş kişiler internete çıkarken, Üniversitenin normal kullanıcılarının bulunduğu ağdan farklı bir ağda olmak kaydıyla, bütün servisleri kullanma hakkına sahiptir.
f) Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmez.
g) İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilmemeli ve indirilmez. Bu konuda gerekli önlemler alınır.
ğ) Üçüncü şahısların internet erişimleri için misafir ağı erişimi verilmelidir.

Sunucu Güvenliği
Madde 9- (1) Sahip olma ve sorumluluklar ile ilgili kurallar aşağıda belirtilmiştir.
a) Üniversitede bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş sistem yöneticisi(leri) sorumludur.
b) Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sistem yöneticisi(leri) tarafından yapılır.
c) Sunuculara ait bilgilerin yer aldığı tablo oluşturulur. Bu tabloda, sunucuların isimleri, ip adresleri ve yeri, ana görevi ve üzerinde çalışan uygulamalar, işletim sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi işlemlerinden sistem yöneticisi(leri)nin isimleri ve telefon numaraları bilgileri yer alır ve bu tablo bir portal üzerinde bulundurulmaz.
ç) Tüm bilgiler, sorumluluk kabul formu(Ek-5) ile sistem yöneticisi olarak belirlenen kişi(ler) tarafından güncel tutulur.

(2) Genel yapılandırma kuralları aşağıda belirtilmiştir.

a) Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri Üniversitenin Bilgi İşlem Daire Başkanlığı talimatlarına göre yapılır.
b) Kullanılmayan servisler ve uygulamalar kapatılır.
c) Sunucu ve Servislere erişimleri Ağ Erişim İzin Talep Formu(EK-1) ile yapılır, kaydedilerek erişim kontrol yöntemleri ile koruma sağlanır.
ç) Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve antivirüs vb. koruma amaçlı yazılımlar sürekli güncellenir. Antivirüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılır. Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, bir onay ve test mekanizmasından, geçirilir sonra uygulanır. Bu çalışmalar için sistem yöneticisi(leri) olmalıdır.
d) Sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmaz. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.
e) Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılır.
f) Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmaz. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanır.
g) Sunucular üzerinde lisanslı yazılımlar kurulur.
ğ) Sunucular fiziksel olarak korunmuş sistem odalarında bulunur.

(3) Sunucu gözlemleme kuralları aşağıda belirtilmiştir.
a) Kritik sistemlerde, uygulamalar kaydedilir ve kayıtlar aşağıdaki gibi saklanır.
b) Günlük backuplar en az 12 gün saklanır.
c) Kayıtlar sunucu üzerinde tutulmalarının yanı sıra ayrı bir sunucuda da saklanır.
ç) Sunucu üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları, vb.) çalıştırılmaz.
d) Kayıtlar sistem yöneticisi(leri) tarafından değerlendirilir ve gerekli tedbirler alınır.
e) Port tarama atakları düzenli olarak yapılır.
f) Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik yapılır.
g) Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilir.
ğ) Denetimler sistem yöneticisi(leri) yönetilir ve belli aralıklarda yapılır.

(4) Sunucu işletim kuralları aşağıda belirtilmiştir.
a) Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, tavan ve taban güçlendirmeleri yapılmış ortamlarda bulundurulur.
b) Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılır.
c) Sistem odalarına giriş ve çıkışlar erişim kontrollüdür.

Ağ Cihazları Güvenliği
Madde 10- (1) Ağ cihazları güvenliği ile ilgili kurallar aşağıda belirtilmiştir.
a) Ağ cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer alır.
b) Yerel kullanıcı hesapları açılmaz. Ağ cihazları kimlik tanımlama için LDAP, RADIUS veya TACAS+ protokollerinden birini kullanır.
c) Yönlendirici ve anahtarlardaki tam yetkili şifre olan 'enable şifresi' kodlanmış formda saklanır. Bu şifrenin tanımlanması Üniversiteun içerisinden yapılır.
ç) Üniversiteun standart olan SNMP community string'leri kullanılır. Bu bilgi sadece sistem yöneticisi(leri) tarafından bilinir.
d) İhtiyaç duyulduğu zaman erişim listeleri eklenmelidir.

e) Yönlendirici ve anahtarlar Üniversitenin yönetim sisteminde olur.
f) Yazılım ve firmware güncellemeleri önce test ortamlarında denenir sonra çalışma günlerinin dışında üretim ortamına taşınır.
g) Cihazlar üzerinde kullanılmayan servisler kapatılır.
ğ) Bilgisayar ağında bulunan kabinetler, aktif cihazlar, ağ kabloları (UTP ve fiber optik aktarma kabloları), cihazların portları etiketlenir.
h) Her bir yönlendirici ve anahtar aşağıdaki uyarı yazısına sahip olmalıdır.
Yönlendiriciye erişen tüm kullanıcıları uyarmalıdır.
"BU CİHAZA YETKİSİZ ERİŞİMLER YASAKLANMIŞTIR. Bu cihaza erişim ve yapılandırma için yasal hakkınız olmak zorundadır. Bu cihaz üzerinde işletilen her komut loglanabilir, buna uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptırım olabilir."

Ağ Yönetimi
Madde 11- (1) Ağ yönetimi ile ilgili kurallar aşağıda belirtilmiştir.
a) Ağ cihazları yönetim sorumluluğu, sunucu ve istemcilerin yönetiminden ayrılır.
b) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılır ve güncellemeler uygulanır.
c) Erişimine izin verilen ağlar, ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilir ve yetkisiz erişimle ilgili tedbirler alınır.
ç) Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanır.
d) Sınırsız ağ dolaşımı engellenir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaçlara göre serbest bırakılır.
e) Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınır.
f) İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınır ve kayıtlar tutulur.
g) Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılır. Üniversite kullanıcılarının bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılır ve ağlar arasında geçiş güvenlik sunucuları (firewall) üzerinden sağlanır.
ğ) Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanır.
h) Bilgisayar ağına bağlı bütün makinelerde kurulum ve yapılandırma parametreleri, Üniversitenin güvenlik ve standartlarıyla uyumlu olmalıdır.
ı) Sistem tasarımı ve geliştirilmesi yapılırken Üniversite tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanılır.
i) İnternet trafiği, İnternet Erişim ve Kullanımı ve ilgili standartlarda anlatıldığı şekilde izlenebilmelidir.
j) Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı şekilde saklanır.
k) Ağ cihazları görevler dışında başka bir amaç için kullanılmaz.
l) Ağ cihazları yapılandırılması Sistem Yöneticisi(leri) tarafından veya Sistem Yöneticisi(leri)nin denetiminde yapılır ve değiştirilir.
m) Ağ dokümantasyonu hazırlanır ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanır.

Uzaktan Erişim
Madde 12- (1) Uzaktan erişim ile ilgili kurallar aşağıda belirtilmiştir.
a) Internet üzerinden Üniversitenin herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya Üniversiteler VPN teknolojisini kullanır. Bu; veri bütünlüğünün korunması, erişim

denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamaktadır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. Protokollerinden birini içermelidir.
b) Uzaktan erişim güvenliği denetlenir.
c) Üniversite çalışanları bağlantı bilgilerini hiç kimse ile paylaşmaz.
ç) Üniversitenin ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olamaz.
d) Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılır.
e) Üniversite ağına uzaktan erişecek bilgisayarların işletim sistemi ve antivirüs yazılımı güncellemeler yapılmış olmalıdır.
f) Üniversiteden ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak, alınır yetkiler ve hesap özellikleri buna göre güncellenir.
g)VPN bağlantısıyla erişim yapacak kullanıcılar VPN erişim formu(EK-3) doldurur.

Kablosuz İletişim
Madde 13- (1) Üniversitenin bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınır.

(2) Bütün kablosuz erişim cihazları sistem yöneticisi(leri) tarafından onaylanmış cihazlar olmalı ve Bilgi İşlemin belirlediği güvenlik ayarlarını kullanmalıdır.

(3) Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.
a) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılır. Bunun için Wi-Fi Protected Access2 (WPA2-Üniversitesal) şifreleme kullanılır. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılır.
b) Erişim cihazlarındaki firmwareler düzenli olarak güncellenir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlamaktadır.
c) Cihaza erişim için güçlü bir parola kullanılır. Erişim parolaları varsayılan ayarda bırakılmaz.
ç) Varsayılan SSID isimleri kullanılmaz. SSID ayarı bilgisi içerisinde Üniversite ile ilgili bilgi olmamalıdır, mesela Üniversite ismi, ilgili bölüm, çalışanın ismi vb.
d) Radyo dalgalarının binanın dışına taşmamasına özen gösterilir. Bunun için çift yönlü antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanır.
e) Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Üniversite kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanır ve Üniversite kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenir.
f) Erişim Cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dâhil olurlar.
g) Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilir ve kullanıcılar tarafından Üniversitenin tüm internet bant genişliğinin tüketilmesi engellenir.
ğ) Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlıdır.
h) Kullanıcı bilgisayarlarında kişisel antivirüs ve güvenlik duvarı yazılımları yüklü olmak zorundadır.
ı) Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenir.

Bilgi Sistemleri Genel Kullanımı
Madde 14- (1) Bilgi sistemlerine sahip olma ve bu sistemleri genel kullanım kuralları aşağıda belirtilmiştir.

a) Üniversitenin güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, Üniversitenin bünyesinde oluşturulan tüm veriler Üniversitenin mülkiyetindedir.
b) Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanamaz.
c) Üniversite, bu çerçevede ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
ç) Üniversite bilgisayarları etki alanına dahil edilir. Etki alanına bağlı olmayan bilgisayarlar yerel ağdan çıkarılır, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi olmaz.
d) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmaz ve kopyalanmaz.
e) Üniversitede Bilgi İşlem Dairesinin bilgisi ve onayı olmadan Üniversite Ağ sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmaz.
f) Birimlerde sistem yöneticisi(leri)nin bilgisi haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilmez.
g) Bilgisayarlara lisanssız program yüklenmez.
ğ) Gerekmedikçe bilgisayar kaynakları paylaşıma açılmaz. Kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilir.

(2) Bilgi sistemleri genel yapılandırması ile ilgili kurallar aşağıda belirtilmiştir.
a) Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Bilgi İşlem Daire Başkanlığı'a da haber verilmelidir.
b) Bütün cep telefonu ve PDA (Personal Digital Assistant) cihazları Üniversitenin ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (kızılötesi, bluetooth, vb) özellikleri aktif halde olmamalıdır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.
c) Kullanıcılar tarafından gönderilen e-postalarda gereğine göre aşağıdaki şekilde bir açıklama yer almalıdır.
"Bu e-posta iş için gönderilenler hariç sadece yukarıda isimleri belirtilen kişiler arasında özel haberleşme amacını taşımaktadır. Size yanlışlıkla ulaşmışsa lütfen gönderen kişiyi bilgilendiriniz ve mesajı sisteminizden siliniz. Namık Kemal Üniversitesi bu mesajın içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmemektedir.
ç) Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve mümkünse dosyalar sıkıştırılmalıdır.

Kriz / Acil Durum
Madde 15- (1) Acil Durum ile ilgili kurallar aşağıda belirtilmiştir.
a) Acil durum sorumluları atanır ve yetki ve sorumlulukları belirlenir ve yazılı hale getirilir.
b) Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınır. Problem durumlarında sistem kesintisiz veya makul kesinti süresi içerisinde felaket ve/veya iş sürekliği merkezi üzerinden çalıştırılabilmelidir.
c) Bilişim sistemlerinin kesintisiz çalışmasının sağlanması için aynı ortamda Kümeleme veya uzaktan kopyalama veya yerel kopyalama veya pasif sistem çözümleri hayata geçirilir. Sistemler tasarlanırken minimum sürede iş kaybı hedeflenir.
ç) Acil durumlarda Üniversite içi işbirliği gereksinimleri tanımlanır.
d) Acil durumlarda sistem kayıtları incelenmek üzere saklanır.
e) Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulur.
f) Yaşanan acil durumlar sonrası süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilir.
g) Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulur ve bu bildirim süreçleri tanımlanmış olur.

ğ) Acil durumlarda Sistem yöneticisi(leri)ne erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere sistem yöneticisi(leri)ne bilgi verilir ve zararın tespit edilerek süratle önceden tanımlanmış felaket kurtarma faaliyetleri yürütülür.
h) Sistem yöneticisi(leri) tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilir.

Fiziksel Güvenlik
Madde 16- (1) Fiziksel Güvenlik ile ilgili kurallar aşağıda belirtilmiştir.
a) Üniversitenin binalarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilir.
b) Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binalarda ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanır ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilir.
c) Üniversite dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili güvenlik görevlileri gözetiminde gerçekleştirilir.
ç) Kritik bilgilerin bulunduğu alanlara girişlerin kontrolü akıllı kartlar veya biyometrik sistemler ile yapılır ve izlenir.
d) Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sistem yöneticisi(leri) tarafından sağlanır.
e) Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanır.
f) Kritik sistemler özel sistem odalarında tutulur.
g) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı, korunur, yangın ve benzer felaketlere karşı koruma altına alınır ve iklimlendirilmesi sağlanır.
ğ) Fotokopi, yazıcı vs. türü cihazlar mesai saatleri dışında kullanıma, kapatılır mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınır.
h) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilir.

Kimlik Doğrulama ve Yetkilendirme
Madde 17- (1) Kimlik Doğrulama ve Yetkilendirme ile ilgili kurallar aşağıda belirtilmiştir.
a) Üniversite sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenir ve yazılı hale getirilir.
b) Üniversite sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanır ve yazılı hale getirilir.
c) Üniversite bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veritabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler, belirlenir, yazılı hale getirilir ve denetim altında tutulur.
ç) Tüm Üniversite sistemleri üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilir ve bu gereksinimler gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilir.
d) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilir.
e) Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak, tutulur, tekrarlanan başarısız erişim istekleri/girişimleri incelenir.
f) Kullanıcılara erişim hakları yazılı olarak beyan edilir.
g) Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılır.
ğ) Sistemler üzerindeki tüm roller, rollere sahip kullanıcılar ve rollerin sistem kaynakları üzerindeki yetkileri uygun araçlar kullanılarak belirli aralıklarla listelenir. Bu listeler yetki

seviyeleri ile karşılaştırılır. Eğer uyumsuzluk varsa dokümanlar ve yetkiler düzeltilerek uyumlu hale getirilir.

Veritabanı Güvenliği

Madde 18- (1) Veritabanı güvenlik kuralları aşağıda belirtilmiştir.

a) Veritabanı sistemleri envanteri yazılı hale getirilir ve bu envanterden sorumlu personel tanımlanır.

b) Veritabanı işletim kuralları belirlenir ve yazılı hale getirilir.

c) Veritabanı sistem kayıtları tutulur ve gerektiğinde idare tarafından izlenir.

ç) Veritabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilir.

d) Veritabanı sistemlerinde tutulan bilgiler sınıflandırılır ve uygun yedekleme oluşturulur, yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli olarak alınması kontrol altında tutulur.

e) Yedekleme planları yazılı hale getirilir.

f) Tutulan log kayıtları en az 2 (iki) yıl süre ile güvenli ortamlarda saklanır.

g) Veritabanı erişimi "Kimlik Doğrulama ve Yetkilendirme" çerçevesinde oluşturulur.

ğ) Hatadan arındırma, bilgileri yedekten dönme kurallarına "Acil Durum Yönetimi" uygun olarak oluşturulur ve yazılı hale getirilir.

h) Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulur.

ı) Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilir.

i) Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulur ve sonrasında ilgili uygulama kontrolleri gerçekleştirilir.

j) Bilgi saklama medyaları Üniversite dışına çıkartılmaz.

k) Sistem dokümantasyonu güvenli şekilde saklanır.

l) İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenir.

m) Veritabanı sunucusu sadece ssh, rdp, ssl ve veritabanının orijinal yönetim yazılımına açık olmalı; bunun dışında ftp, telnet vb. gibi açık metin şifreli bağlantılara kapalı olmalıdır. Ancak ftp, telnet vb. açık metin şifreli bağlantılar veri tabanı sunucudan dışarıya yapılabilir.

n) Uygulama sunucularından veritabanına rlogin vb. şekilde erişememelidir.

o) Veritabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak Üniversitenin kasasında saklanır ve gereksiz yere açılmaz. Zarfın açılması durumunda firma yetkilileri de bilgilendirilir.

ö) Arayüzden gelen kullanıcılar bir tabloda, saklanır, bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmalıdır.

p) Veritabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak. bağlanılır. Root veya admin şifresi tanımlı kişi/kişilerde olur.

r) Bağlanacak kişilerin kendi adına kullanıcı adı verilir ve yetkilendirme yapılır.

s) Bütün kullanıcıların yaptıkları işlemler kaydedilir.

ş) Veritabanı yöneticiliği yetkisi sadece bir kullanıcıda olur.

t) Veritabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenir.

u) Veritabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar tesis edilir.

ü) Veritabanı sunucularına ağ erişim formu(EK-1) yetkilendirilmiş kullanıcılar erişir.

v) Veritabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp sorgu yapamaz. İstekler arayüzden sağlanır.(örnek; Kullanıcılar tablolardan "select" sorgu cümleciklerini yazarak sorgulama yapmamalıdır)

y) Veritabanı sunucularına giden veri trafiği mümkünse Şifrelenir.(Ağ trafiğini dinleyen casus yazılımların verilere ulaşamaması için)
z) Bütün şifreler düzenli aralıklarla değiştirilir. (Detaylı bilgi için Parolaya bakılmalıdır.)
aa) Veritabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için de geçerlidir.

Değişim Yönetimi
Madde 19- (1) Değişim Yönetimi ile ilgili kurallar aşağıda belirtilmiştir.
a) Bilgi sistemlerinde sistem yöneticisi(leri) ve yetki seviyeleri yazılı hale getirilir.
b) Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilir.
c) Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenir ve yazılı hale getirilir.
ç) Değişiklikler gerçekleştirilmeden önce Sistem yöneticisi(leri) ve ilgili diğer yöneticilerin onayı alınır.
d) Tüm sistemlere yönelik yapılandırma dokümantasyonu, oluşturulur, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilir.
e) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanır ve ilgili yöneticiler tarafından onaylanması sağlanır.
f) Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilir.
g) Teknoloji değişikliklerinin Üniversitenin sistemlerine etkileri belirli aralıklarla gözden geçirilir ve yazılı hale getirilir.

Bilgi Sistemleri Yedeklemesi
Madde 20- (1) Bilgi Sistemleri Yedeklemesi ile ilgili kurallar aşağıda belirtilmiştir.
a) Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerini ve kurumsal veriler düzenli olarak yedeklenir.
b) Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde yedekleri alınır.
c) Veriler offline ortamlarda en az 1 (bir) yıl süreyle saklanır.
ç) Kurumsal kritik verilerin saklandığı veya sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılır ve yedekleme ihtiyacı bakımından sınıflandırılarak yazılı hale getirilir.
d) Düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamaların çalıştığı ve yedeği alınacak dizin, dosya bilgi sistemlerinde sistem yöneticisi(leri) ve yetki seviyeleri yazılı hale getirilir.
e) Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanır ve atamalar yapılır.
f) Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenir ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulur.
g) Yedek ünite üzerinde gereksiz yer tutmamak amacıyla, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dâhil edilmez.
ğ) Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilir ve güncellenir.
h) Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenir.
ı) Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilir ve temin edilir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilir.

i) Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanır.
j) Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dâhilinde tamamlanması gerekir.
k) Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanır.
l) Yedekleme Standardı ile doğru ve eksiksiz yedek kayıt kopyaları bir felaket anında etkilenmeyecek bir ortamda bulundurulur.
m) Veri Yedekleme Standardı, yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği belirlenir. Yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanır ve işlerliği periyodik olarak gözden geçirilir.

Personel Güvenliği
Madde 21- (1) Personel Güvenliği ile ilgili kurallar aşağıda belirtilmiştir.
a) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılır.
b) Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilir ve alınır.
c) Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi, araştırılır, beyan edilen akademik ve profesyonel bilgiler teyit, edilir, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorulması sağlanır.
ç) Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenir.
d) Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanır.
e) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenir.
f) İş tanımı değişen veya Üniversiteden ayrılan kullanıcıların erişim hakları kaldırılır.
g) Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundururlar.
ğ) Üniversite bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak, yapılır, bütçe, ayrılır, eğitimlere katılım sağlanır ve eğitim etkinliği değerlendirilir.
h) Yetkiler, "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı", rollerin ve sorumlulukların paylaştırılması ile ilgilidir. Bu paylaşım ile kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılmalıdır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla yetkiyle donatılmamasıdır. Sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmalıdır.
ı) Çalışanlar, kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler, görev ve yetkileri hakkında periyodik olarak eğitilir. Yeni işe alınan elemanlar için de bu eğitim, uyum süreci sırasında verilir.
i) Çalışanların güvenlik ile ilgili aktiviteleri izlenir.
j) Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi, sağlanır varsa devam eden sorumluluklar kayıt altına alınır.

Bakım
Madde 22- (1) Bakım ile ilgili kurallar aşağıda belirtilmiştir.
a) Üniversite sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınır. Bunun için gerekli anlaşmalar için yıllık bütçe ayrılır.

b) Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanır.
c) Firma teknik destek elemanlarının bakım yaparken "Namık Kemal Üniversitesi Bilgi Güvenliği" uygun davranmaları sağlanır ve kontrol edilir.
ç) Sistem üzerinde yapılacak değişiklikler ile ilgili olarak "Değişim Yönetimi" ve ilişkili standartlar uygulanır.
d) Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenir.
e) Sistem bakımlarının ilgili standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik uygunluk ve güvenlik testleri yapılır.
f) Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda "Namık Kemal Üniversitesi Bilgi Güvenliği Yönergesi" uyarınca hareket edilir

Yazılım Geliştirme
Madde 23- (1) Yazılım Geliştirme ile ilgili kurallar aşağıda belirtilmiştir.
a) Sistem yazılımında mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.
b) Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.
c) İhtiyaçlar, uygun bir şekilde tanımlanmalıdır.
ç) Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.
d) Üniversite içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.
e) Üniversitede kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.
f) Hazırlanan sistemler mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları belgelenerek onaylanmalıdır.
g) Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.
ğ) Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.
h) Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.
ı) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.
i) Yazılımlar sınıflandırılmalı / etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

Belgelendirme
Madde 24- (1) Belgelendirme ile ilgili kurallar aşağıda belirtilmiştir.
a) Bilişim sisteminin yapısı ile bütün iş ve işlemler açıkça belgelenmeli ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir durumda olmalıdır.
b) İş akışları uygun şekilde belgelenmelidir.
c) Belgeleme, tarih belirtilerek yapılmalı ve yedek kopyaları güvenli bir yerde muhafaza edilmelidir.
ç) Girdi türleri ve girdi form örnekleri belgelenmelidir.
d) Ana dosyalar ile diğer dosyaların içerik ve şekilleri belgelenmelidir.
e) Çıktı form örnekleri ve çıktıların kimlere dağıtılacağı belgelenmelidir.
f) Programların nasıl test edildiği ve test sonuçları belgelenmelidir.
g) Bütün program değişikliklerinin detayları belgelenmelidir.

ÜÇÜNCÜ BÖLÜM
Çeşitli Hükümler

Yürürlük
Madde 26- (1) Bu Yönerge Rektörün onayı ile yürürlüğe girer.

Yürütme
Madde 27- (1) Bu yönerge hükümlerini Rektör yürütür.