T.C. BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI
BİLGİ GÜVENLİĞİ YÖNERGESİ

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç

MADDE 1 - (1) Bu yönergenin amacı; Üniversite ile ilgili olarak sunucu ve kullanıcı açısından bilginin gizlilik, bütünlük ve erişilebilirliğinin tüm tehditlerden korunması için gerekli şebeke ve bilgi güvenliğinin sağlanmasına yönelik uyulacak usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu yönerge, Bandırma Onyedi Eylül Üniversitesi akademik ve idari teşkilatı kapsamındaki tüm 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 ve kısaltmalar

MADDE 4 - (1) Bu yönergede geçen;

a) Bilgi: Verilerin anlam kazanmış biçimini,

b) Daire Başkanlığı: Bilgi İşlem Dairesi Başkanlığını,

c) DMZ: Üniversite içi ağı ile Üniversite dışı ağı birbirinden ayıran bölgeyi,

d) Erişim: Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını,

e) Firmware: Sayısal veri işleme yeteneği bulunan her türlü donanımın kendisinden beklenen işlevleri yerine getirilebilmesi için kullandığı yazılımları,

f) IP: Bilgisayar ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alış verişi yapmak için kullandıkları adresi,

g) 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 sağlamayı,

h) İnternet ortamı: Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,

i) İnternet ortamında yapılan yayın: İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri,

j) İstemci: Sunucuların verdiği hizmeti alan bilgisayar sistemini,

k) Kullanıcı: Üniversite bilgi sistemlerini kullanan tüm kişileri,

l) MAC adresi: Bir ağ cihazının tanınmasını sağlayan kendisine özel adresi,

m) RADIUS “Remote Authentication Dialin User Service”: Sunuculara uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan internet protokolünü,

n) Rektör: Bandırma Onyedi Eylül Üniversitesi Rektörünü,

o) Risk: Üniversitenin bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörleri,

p) Sahte e-posta: Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenini kazanma ve kişisel bilgilerine “tamamen yasadışı yoldan” erişme amaçlı e-postayı,

q) Sistem yöneticisi: Bilgi işlem daire başkanlığı bünyesinde görevlendirilmiş yetkin bilgi sistemleri yöneticisini,

r) SNMP: Bilgisayar ağları üzerindeki birimleri denetlemek amacıyla tasarlanmış protokolü,

s) Spam: Yetkisiz ve/veya istenmeyen reklam içerikli e-postaları,

t) SSL “Secure Socket Layer”: Ağ üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş güvenlik protokolünü,

u) Sunucu: İstemcilerden gelen isteklere hizmet verebilen bilgisayar sistemini,

v) Şifreleme: Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan özel bir algoritmayı,

w) Uygulama sunucusu: Üç katmanlı uygulamaların bir parçası olarak dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımını,

x) Uzaktan erişim: İnternet, telefon hatları veya kiralık hatlar vasıtası ile Üniversitenin ağına erişilmesini,

y) Üniversite: Bandırma Onyedi Eylül Üniversitesini,

z) Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,

aa) Veritabanı: Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğunu,

bb) 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 grubunu,

cc) VPN: Bir ağa güvenli bir şekilde, uzaktan erişimi sağlayan teknolojiyi,

dd) X.509/LDAP “Light weight Directory Access Protocol”: Aktif dizin ve e-posta gibi programlardan bilgi aramak için kullanılan bir internet protokolünü,

ee) Yayın: İnternet ortamında yapılan yayını,

ff) Yedekleme: Ekipmanın bozulması durumu düşünülerek dosyaların ve/veya veritabanının başka bir yere kopyalanması işlemini,

gg) Yetkilendirme: Sisteme giriş izni verilmesi olup çok kullanıcılı sistemlere kişilerin girebilmesi ve sistemde işlemler yapabilmesi için sistem yöneticisi tarafından sınırları belirli izinlerin verilmesini,

hh) Yönerge: T.C. Bandırma Onyedi Eylül Üniversitesi Bilgi İşlem Daire Başkanlığı Bilgi Güvenliği Yönergesini,

ii) Zincir e-posta: Bir kullanıcıya gelen şans ve para kazanma yöntemleri gibi bir içeriğe sahip epostanın art arda diğer kullanıcılara gönderilmesini

İfade eder.

İKİNCİ BÖLÜM

Bilgi Güvenliği

E-posta

MADDE 5 - (1) E-posta hesabı;

a) İlgili formu dolduran kişilerin talebi üzerine e-posta adresi kullanıcı hesabı oluşturulabilir. Kullanıcı adı ve parolası okunabilen, açık eden veya güvenlik açığı oluşturan POP3, SMTP, HTTP vb. protokolleri kullanılmaz.

b) 6 ay süreyle kullanılmadığında kapatılabilir.

c) Yetkili kişiler, kurumsal e-postaları hukuksal açıdan gerekli gördüklerinde önceden haber vermeksizin denetleyebilir.

d) Kişisel amaçlar için veya ticari ve kâr amaçlı olarak kullanılamaz.

e) Uygunsuz verilerin "siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb." paylaşımında kullanılamaz.

f) Taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderiminde kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında ilgili birime haber verilir.

g) Tehdit, hakaret, küfür, iftira, genel ahlaka aykırılık gibi suç içeren mesajların yollanmasından hesap sahibi sorumlu tutulur.

h) Mesajların, gönderilen kişi dışında başkalarına ulaşmaması kullanıcının sorumluluğundadır.

i) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postaları cevaplandırılmaz. Virüs, solucan, truva atı, trojan, malware veya diğer zararlı kodlar bulaşmış e-postaların antivirüs yazılımları vasıtasıyla içeriği korunacak şekilde virüslerden temizlenmesi sağlanır.

j) Donanım ve yazılım sistemleri yetkisiz erişimlere karşı korunur ve parolalar, yetkisiz ikinci bir şahsa verilemez.

k) Parola güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden hesap sahibi sorumlu olup e-posta ve mesajların yetkisiz kişiler tarafından görülmesini ve okunmasını engelleyici parola kullanır ve bunları belirli aralıklarla değiştirir.

l) Kullanıcı kodu veya parolası isteyen e-postalar geldiğinde bunlarla ilgili herhangi bir işlem yapılmaksızın ilgili birime haber verilir.

m) Parolaların başkası tarafından ele geçirildiği fark edildiğinde gecikmeden ilgili birime haber verilir.

n) Kaynağı bilinmeyen e-postaların ekinde gelen dosyalar kesinlikle açılmaz. Bu tür tehdit içeren e-postalar, zincir mesajları ve mesajlara iliştirilmiş dosyalar başkalarına iletilmez ve ilgili birime haber verilir.

o) Kullanıcı, kurumsal bilgi talep eden mesajları, Üniversite iş akışını aksatmaması için cevaplandırır.

p) Gönderilen mesajlarda veya iliştirilen öğelerde Üniversite ile ilgili gizli bilgilere yer verilmez.

Parola

MADDE 6 - (1) Parololar;

a) Sistem hesaplarına ait "root, administrator, enable, vs." parolalar en geç 6 "altı" ayda bir değiştirilir.

b) Kullanıcı “e-posta, web, masaüstü bilgisayar, vs” hesaplarına ait parolalar en geç 45 ”kırk beş” günde bir değiştirilir.

c) Sistem Yöneticisi, sistem ve kullanıcı hesapları için farklı parolalar kullanır.

d) Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmez.

e) Parolalar başkası ile paylaşılmaz, kâğıtlara ya da elektronik ortamlara yazılmaz.

f) Kullanıcı adı ve parolası, kullanıcıya ait ve / veya kurum tarafından tahsis edilen cihazların dışında kullanılamaz. Ayrıca en fazla 5 cihaz eş zamanlı kullanılabilir.

g) Domaine dahil olan bilgisayarlarda kullanıcılar, sadece kendilerine tanımlı olan bilgisayarlarda oturum açabilir.

(2) Parola;

a) En az 8 haneli olmalıdır.

b) İçerisinde en az 1 tane harf bulunmalıdır. (a, b, C...)

c) İçerisinde en az 1 tane rakam bulunmalıdır. (1, 2, 3...)

d) İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !, . v.b.)

e) Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, ababab...)

f) Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,1234,zxcvb...)

g) Kullanıcıya ait anlam ifade eden aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb. gibi kelimeler içermemelidir.

(3) Şifrenin korunması konusunda aşağıdaki hususlara uyulur:

a) Bütün parolalar Üniversiteye ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.

b) Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki “parola hatırlama” seçeneği kullanılmamalıdır.

(4) Uygulama geliştirme standartları konusunda aşağıdaki hususlara uyulur:

a) Bireylerin ve grupların kimlik doğrulaması işlemini desteklemelidir.

b) Parolalar metin olarak veya kolay anlaşılabilir formda saklanmamalıdır.

c) Parolalar, şifrelenmiş olarak saklanmalıdır.

d) En az RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

Antivirüs

MADDE 7 - (1) Antivirüs konusunda aşağıdaki hususlara uyulur:

a) Üniversitenin tüm istemci ve sunucularında antivirüs yazılımı olacaktır. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine, istisna olarak antivirüs yazılımı yüklenmeyebilir.

b) İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılabilir.

c) Sistem yöneticileri, antivirüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.

d) Kullanıcı antivirüs yazılımını bilgisayarından kaldıramaz.

e) Sunucuların internete sürekli bağlı olması, veri tabanlarının otomatik olarak güncellenmesi sağlanacak ve etki alanına bağlı istemcilerin antivirüs güncellemeleri antivirüs sunucusu tarafından otomatik olarak yapılacaktır.

f) Etki alanına dâhil olmayan kullanıcılar da antivirüs güncellemesi yapmaktan sorumlu olup, sistem yöneticileri herhangi bir sakıncalı durumu tespit ettiklerinde bu bilgisayarları ağdan çıkartabilecektir.

g) Bilinmeyen veya şüpheli kaynaklardan gelen dosyalar indirilemez.

h) Üniversitenin ihtiyacı haricinde kullanıcıya tahsis edilen cihazlarda okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilir.

i) Optik media ve harici veri depolama cihazları kullanmadan önce antivirüs kontrolünden geçirilir.

j) Sunucular üzerindeki 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 ile korunacaktır.

İnternet erişim ve kullanımı

MADDE 8 - (1) İnternet erişim ve kullanımı konusunda aşağıdaki hususlara uyulur:

a) Üniversitenin bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvarları üzerinden internete çıkılır. Ağ güvenlik duvarı, Üniversitenin ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında Üniversitenin karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.

b) Üniversitenin uygulamaları doğrultusunda içerik filtreleme sistemleri kullanılır. Kurumsal kullanıma uygun olmayan ve yasaklı pornografi, oyun, kumar, şiddet, torrent vs. içeren sitelere erişim engellenir.

c) Üniversitenin ihtiyacı doğrultusunda saldırı tespit ve önleme sistemleri kullanılır.

d) Üniversitenin ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılır. İnternete giden ve gelen bütün trafik virüslere karşı taranır.

e) Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kuralları güncel olarak uygulanır.

f) Misafir kullanıcılar internete çıkarken, Üniversitenin normal kullanıcılarının bulunduğu ağdan farklı bir ağda olmak kaydıyla, bütün servisleri kullanma hakkına sahiptir.

g) Üçüncü şahısların internet erişimleri için misafir ağı erişimi verilir.

h) Bu yönergenin ekinde bulunan "6698 Sayılı Kişisel Verilerin Korunması Kanunu ve Bu Kanun Kapsamındaki Haklarınız ile İlgili Beyan ve Onay Formu" yeni başlayan personeller dahil tüm personele onaylatılır. İmtina eden personelin Bilgi İşlem Daire Başkanlığı hizmetlerinden yararlanması engellenir.

Sunucu güvenliği

MADDE 9 - (1) Sahip olma ve sorumluluklar konusunda aşağıdaki hususlara uyulur:

a) Üniversitemizin kontrolü altında bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş sistem yöneticileri sorumludur.

b) Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları ve güncellemeleri sadece sistem yöneticileri tarafından yapılır.

(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 erişimler "Ağ Erişim İzin Talep Formu" ile yapılır, kaydedilerek erişim kontrol yöntemleri ile koruma sağlanır.

d) 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 sistem yöneticileri kontrolünde yapılır.

e) Sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmaz. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.

f) Ayrıcalıklı bağlantılar teknik olarak güvenli, SSL, IPSec VPN gibi şifrelenmiş ağ kanalları üzerinden yapılır.

g) Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmaz. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanır.

h) Sunucular üzerinde lisanslı yazılımlar kurulur.

i) Sunucular fiziksel olarak korunmuş sistem odalarında bulunur.

(3) Kritik sistemlerde, sunucu gözlemleme kuralları ile uygulamaların kaydedilmesi ve kayıtların saklanması aşağıdaki şekilde yapılır;

a) Günlük backuplar en az 10 gün saklanır.

b) Kayıtlar sunucu üzerinde tutulmalarının yanı sıra ayrı bir sunucuda da saklanır.

c) Malware, spyware, warez ve hack programları gibi zararlı yazılım programları çalıştırılamaz.

d) Kayıtlar sistem yöneticileri 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.

(4) Sunucu işletim kuralları aşağıda belirtilmiştir.

a) Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, sunucu barındırmaya uygun 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 konusunda aşağıdaki hususlara uyulur:

a) Ağ cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer alır.

b) Yönlendirici ve anahtarlardaki tam yetkili şifre olan 'enable şifresi' kodlanmış formda saklanır. Bu şifrenin tanımlanması Üniversite içerisinden yapılır.

c) Üniversite'de standart olan SNMP community string'leri kullanılır. Bu bilgi sadece sistem yöneticileri tarafından bilinir.

d) İhtiyaç duyulduğu zaman erişim listeleri eklenmelidir.

e) Yönlendirici ve anahtarların temini ve ağa dahil edilmesi Üniversitemiz Bilgi İşlem Daire Başkanlığı kontrolünde yapılır.

f) Yazılım ve firmware güncellemeleri önce test ortamlarında denenir sonra çalışma günlerinin dışında üretim ortamına taşınır.

g) Cihazlar üzerinde kullanılmayan servisler kapatılır.

h) Bilgisayar ağında bulunan kabinetler, aktif cihazlar, UTP ve fiber optik aktarma kabloları gibi ağ kabloları, cihazların portları etiketlenir.

i) Her bir yönlendirici ve anahtar aşağıdaki uyarı yazısına sahip olmalıdır. Yönlendiriciye erişen tüm kullanıcıları uyarmalıdır.

"Bu cihaza yetkisiz erişimler yasaklanmıştır. 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 konusunda aşağıdaki hususlara uyulur:

a) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılır ve güncellemeler uygulanır.

b) Erişimine izin verilen ağlar, ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilir ve yetkisiz erişimle ilgili tedbirler alınır.

c) İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınır ve kayıtlar tutulur.

d) 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 sunucusu firewall üzerinden sağlanır.

e) Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanır.

f) Bilgisayar ağına bağlı bütün makinelerde kurulum ve yapılandırma parametreleri, Üniversitenin güvenlik ve standartlarıyla uyumlu olmalıdır.

g) Sistem tasarımı ve geliştirilmesi yapılırken Daire Başkanlığınca onaylanmış olan ağ ara yüzü ve protokoller kullanılır.

h) İnternet trafiği, internet erişim ve kullanımı ilgili mevzuata uygun olarak izlenir.

i) Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı şekilde saklanır.

j) Ağ cihazları görevler dışında başka bir amaç için kullanılmaz.

k) Ağ cihazları yapılandırılması sistem yöneticileri tarafından veya sistem yöneticilerinin denetiminde yapılır ve değiştirilir.

l) Ağ dokümantasyonu hazırlanır ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanır.

Uzaktan erişim

MADDE 12 - (1) Uzaktan erişim konusunda aşağıdaki hususlara uyulur:

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.

d) Üniversitenin ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olamaz.

e) Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılır.

f) Üniversite ağına uzaktan erişecek bilgisayarların işletim sistemi ve antivirüs yazılımı güncellemeler yapılmış olmalıdır.

g) Üniversiteden ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri sistem üzerinden otomatik olarak alınır, yetkiler ve hesap özellikleri buna göre güncellenir.

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 yöneticileri tarafından onaylanmış cihazlar olmalı ve Bilgi İşlemin belirlediği güvenlik ayarlarını kullanmalıdır.

(3) Kablosuz iletişim konusunda aşağıdaki hususlara uyulur:

a) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılır. Bunun için güncel şifreleme sistemleri 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.

d) 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.

e) Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilebilir ve kullanıcılar tarafından Üniversitenin tüm internet bant genişliğinin tüketilmesi engellenebilir.

f) Kullanıcı bilgisayarlarında kişisel antivirüs ve güvenlik duvarı yazılımları yüklü olmak zorundadır.

g) Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenir.

Bilgi sistemleri genel kullanımı

Madde 14 - (1) Bilgi sistemleri genel kullanımı konusunda aşağıdaki hususlara uyulur:

a) Üniversitenin otomasyonlarında oluşturulan tüm veriler Üniversitenin mülkiyetindedir. Yetkisiz kişilerle paylaşılamaz.

b) Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanamaz.

c) Üniversite, bu çerçevede ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.

d) Üniversite bilgisayarları etki alanına dahil edilir. Etki alanına bağlı olmayan bilgisayarlar yerel ağdan çıkarılır.

e) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmaz ve kopyalanmaz.

f) Üniversitede Bilgi İşlem Dairesinin bilgisi ve onayı olmadan Üniversitenin web hosting, e-posta servisi vb. ağ sisteminde sunucu nitelikli bilgisayar bulundurulmaz.

g) Birimlerde sistem yöneticilerinin bilgisi haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilmez.

h) Bilgisayarlara lisanssız program yüklenmez.

i) Gerekmedikçe bilgisayar kaynakları paylaşıma açılmaz. Kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilir.

(2) Bilgi sistemleri genel yapılandırması konusunda aşağıdaki hususlara uyulur:

a) Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Bilgi İşlem Daire Başkanlığı'na da haber verilmelidir.

b) Bütün mobil cihazlar Üniversitenin ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda, kablosuz erişim sağlayan "kızılötesi, bluetooth, vb." özellikleri aktif halde olmamalıdır ve mümkünse antivirüs programları ile yeni nesil virüslere karşı korunmalıdır.

c) Kullanıcılar tarafından gönderilen e-postalarda aşağıdaki şekilde bir açıklama yer almalıdır.

''Bu e-posta'nın içerdiği bilgiler ekleri de dahil olmak üzere gizlidir. Üniversitenin onayı olmaksızın içeriği kopyalanamaz, üçüncü kişilere açıklanamaz veya iletilemez. Bu mesajın gönderilmek istendiği kişi değilseniz ya da bu e-posta'yı yanlışlıkla aldıysanız lütfen yollayan kişiyi haberdar ediniz ve mesajı sisteminizden derhal siliniz. Bandırma Onyedi Eylül Üniversitesi bu mesajın içerdiği bilgilerin doğruluğu veya eksiksiz olduğu konusunda bir garanti vermemektedir. Bu nedenle, bilgilerin ne şekilde olursa olsun içeriğinden, iletilmesinden, alınmasından, saklanmasından Üniversitenin sorumluluğu bulunmamaktadır. Bu mesajın içeriği yazarına ait olup, Üniversitenin görüşlerini içermeyebilir.''

d) 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) Kriz / acil durum hallerinde aşağıdaki hususlara uyulur:

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 çalıştırılabilir.

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.

d) Acil durumlarda Üniversite içi işbirliği gereksinimleri tanımlanır.

e) Acil durumlarda sistem kayıtları incelenmek üzere saklanır.

f) Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulur.

g) Yaşanan acil durumlar sonrası süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilir.

h) Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulur ve bu bildirim süreçleri tanımlanmış olur.

i) Acil durumlarda Sistem yöneticilerine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere sistem yöneticilerine bilgi verilir ve zararın tespit edilerek süratle önceden tanımlanmış felaket kurtarma faaliyetleri yürütülür.

j) Sistem yöneticileri tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilir.

Fiziksel güvenlik

MADDE 16 - (1) Fiziksel güvenlik konusunda aşağıdaki hususlara uyulur:

a) Üniversite dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili görevliler gözetiminde gerçekleştirilir.

b) Kritik bilgilerin bulunduğu alanlara girişlerin kontrolü akıllı kartlar veya biyometrik sistemler ile yapılır ve izlenir.

c) Kritik sistemler sistem odalarında tutulur.

d) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı, korunur, yangın ve benzer felaketlere karşı koruma altına alınır ve iklimlendirilmesi sağlanır.

e) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilir.

Kimlik doğrulama ve yetkilendirme

MADDE 17 - (1) Kimlik doğrulama ve yetkilendirme konusunda aşağıdaki hususlara uyulur:

a) Üniversite sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenir.

b) Üniversite sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanır.

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 yetkileri belirlenir, denetim altında tutulur.

d) Üniversite sistemleri üzerindeki kullanıcıların, kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar da dahil tüm kullanım hakları periyodik olarak gözden geçirilir ve bu gereksinimler gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilir.

e) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilir.

f) Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulur, tekrarlanan başarısız erişim istekleri/girişimleri incelenir.

g) Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılır.

h) 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 güvenliği konusunda aşağıdaki hususlara uyulur:

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.

d) Veritabanında kritik verilerin okunması, değiştirilmesi, silinmesi, eklenmesine yönelik her türlü erişim işlemleri kaydedilir.

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

f) Tutulan log kayıtları en az 1 "bir" yıl süre ile güvenli ortamlarda saklanır.

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

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

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

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

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

l) Bilgi saklama medyaları Üniversite dışına çıkartılmaz.

m) Sistem dokümantasyonu güvenli şekilde saklanır.

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

o) 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.

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

q) Veritabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak bağlanılır. Root veya admin şifresi tanımlı kişi veya kişilerde bulunur.

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

s) Bütün kullanıcıların yaptıkları işlemler kaydedilir.

t) Veritabanı yöneticiliği yetkisi sistem sorumlusu veya sorumlularında olur.

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

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

w) Veritabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp "select vb." sorgu cümleciklerini yazarak sorgulama yapamaz. İstekler arayüzden sağlanır.

x) Veritabanı sunucularına giden veri trafiği mümkünse ağ trafiğini dinleyen casus yazılımların verilere ulaşamaması için şifrelenir.

y) Bütün şifreler, bu yönergenin 6. maddesinde belirtilen esaslar çerçevesinde düzenli aralıklarla değiştirilir.

z) Veritabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için de geçerlidir.

Değişim yönetimi

MADDE 19 - (1) Değişim yönetimi konusunda aşağıdaki hususlara uyulur:

a) Değişiklikler gerçekleştirilmeden önce sistem yöneticileri ve ilgili diğer yöneticilerin onayı alınır.

b) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanır ve ilgili yöneticiler tarafından onaylanması sağlanır.

c) Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilir.

d) Teknoloji değişikliklerinin Üniversitenin sistemlerine etkileri belirli aralıklarla gözden geçirilir.

Bilgi sistemleri yedeklemesi

MADDE 20 - (1) Bilgi sistemleri yedeklemesi konusunda aşağıdaki hususlara uyulur:

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.

d) Kurumsal kritik verilerin saklandığı veya sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılır ve yedekleme ihtiyacı bakımından sınıflandırılarak 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.

h) Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilir ve güncellenir.

i) Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenir.

j) Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilir ve temin edilir.

k) Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilir.

l) Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanır.

m) Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dâhilinde tamamlanması gerekir.

n) Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanır.

o) Yedekleme Standardı ile doğru ve eksiksiz yedek kayıt kopyaları bir felaket anında etkilenmeyecek bir ortamda bulundurulur.

p) 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 konusunda aşağıdaki hususlara uyulur:

a) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılır.

b) Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanır.

c) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenir.

d) İş tanımı değişen veya Üniversiteden ayrılan kullanıcıların erişim hakları kaldırılır.

e) Üniversite bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapılır, eğitimlere katılım sağlanır ve eğitim etkinliği değerlendirilir.

f) 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.

g) Çalışanlar, bilgi güvenliği sorumlulukları, riskler, görevleri ve yetkileri hakkında periyodik olarak eğitilir. Yeni işe alınan elemanlar için de bu eğitim, uyum süreci sırasında verilir.

h) Çalışanların güvenlik ile ilgili aktiviteleri izlenir.

i) 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 konusunda aşağıdaki hususlara uyulur:

a) Üniversitenin donanımlarının, uygulama yazılımlarının, paket yazılımlarının ve işletim sistemlerinin tamamı 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 bu yönergeye uygun davranmaları sağlanır ve kontrol edilir.

d) Sistem bakımlarından sonra bir güvenlik açığından şüphelenilmesi durumunda bu yönerge uyarınca hareket edilir.

Yazılım geliştirme

MADDE 23 - (1) Yazılım geliştirme konusunda aşağıdaki hususlara uyulur:

a) Sistem yöneticisi uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.

b) İhtiyaçlar, uygun bir şekilde tanımlanmalıdır.

c) Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.

d) Üniversitede kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.

e) Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.

f) Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.

g) Yeni yazılımların dağıtımı ve uygulanması Daire Başkanlığı kontrolünde yapılmalıdır.

ÜÇÜNCÜ BÖLÜM

Çeşitli Hükümler

Yürürlük

MADDE 26 - (1) Bu yönerge Rektör onayı ile yürürlüğe girer.

Yürütme

MADDE 27 - (1) Bu yönerge hükümlerini Rektör yürütür.