Misyon

Eğitim-öğretim, araştırma-geliştirme faaliyetleri ile idari ve yönetimsel işlevler için gelişen bilgi teknolojilerini kullanıma sunmak, Üniversitemiz akademik ve idari personel ile öğrencilerin gereksinim duyacağı bilişim hizmetleri ve servislerinin karşılanmasında ihtiyaç duyulan yazılımsal ve donanımsal çözümleri üretmek, temin etmek ve bu amaçla yeni bilişim teknolojilerini üniversitemize kazandırarak etkin ve verimli bir şekilde kullanımını ve devamlılığını sağlamaktır.

Vizyon

Bilişim teknolojileri konusundaki gelişmeleri yakından izleyerek; Üniversitemizin teknolojik alt yapısını sürekli geliştirmek, tüm birimlerin yaygın olarak faydalanılmasını sağlamak, bilişim hizmetlerinin üretilmesi, yürütülmesi ve sunumunda teknolojik alt yapısı ve hizmet kalitesi açısından Üniversitemizin dünyadaki nitelikli üniversiteler arasında yer almasını sağlamak için, bilişim alanında gerekli desteği eksiksiz sağlayabilen bir birim olmaktır.

Genel Hükümler

Madde 1 - Bu politikalar; Üniversitedeki tüm bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik açısından güvenliğinin sağlanmasını amaçlamaktadır.

Madde 2 - Bu dokümanın kapsamı, bilişim altyapısını ve bunları kullanmakta olan tüm birimleri ve bağlı kuruluşları, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

Madde 3 - Bu Yönergenin hazırlanmasında, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve " Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği" esas alınmıştır.

Uygulamalar

Madde 4 - Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla Nuh Naci Yazgan Üniversitesi bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının risk seviyesini, kabul edilebilir risk seviyesinin altında tutmak hedeflenmektedir. Bu hedeflerin gereği olarak ;

4.1. Bilgi Güvenliği Politikaları kurumun güvenilirliğini ve itibarını korumayı sağlar.
4.2. Bilgi Güvenliği Politikaları kurumun ve paydaşlarının bilgi varlıklarına güvenli bir şekilde erişimini sağlar.

4.3. Bilgi Güvenliği Politikası kurumun ve paydaşlarının bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi sağlar.
4.4. Bilgi güvenliğinin ihlali durumunda gerekli görülen yaptırımları uygular.
4.5. Tabi olduğu ulusal ve uluslararası yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlar.
4.6. İş/Hizmet sürekliliğine karşı bilgi güvenliği tehditlerinin etkisini azaltır ve işin sürekliliği ile sürdürülebilirliğini sağlar.
4.7. Çeşitli kontrollerle bilgi güvenliği seviyesini korumayı ve iyileştirmeyi taahhüt eder.
4.8. NNYÜ/NET kullanıcıları bilgi güvenliği politikalarına, talimat ve prosedürlerine uymakla yükümlüdür.
4.9. NNYÜ/NET kullanıcılarını içeriden veya dışarıdan gelebilecek tehditlere karşı korumak, üretilen veya kullanılan bilgilerin gizliliğini güvence altına alarak NNYÜ/NET'in imajını korumakla yükümlüdür.
4.10. Üçüncü taraflarla yapılan sözleşmelerde güvenlik prosedürleri belirlenir.
4.11. Bilgi Güvenliği prosedürlerini yerine getirerek personelin bilgi güvenliği farkındalıklarını artırır.
4.12. Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlar.
4.13. NNYÜ/NET kullanıcıları, kritiklik düzeylerine göre işlediği bilgiyi yedekler.
4.14. NNYÜ/NET kullanıcıları, bilgi güvenliği ihlal olaylarını bilgi güvenliği yetkilisine bildirmeli, raporlamalı ve bu ihlalleri engelleyecek önlemleri almalıdır.
4.15. NNYÜ/NET bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.
4.16. Hizmet alanlara, verenlere ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği, bütünlüğü ve erişilebilirliği her durumda güvence altına alınır.
4.17. Bilgi güvenliği politikalarının yürütülmesi Bilgi İşlem Dairesi Başkanlığı tarafından yerine getirilir.
4.18. NNYÜ/NET kullanıcıları bilgi güvenliği kapsamında aşağıda belirtilen kurallara uymakla yükümlüdür:

a) NNYÜ/NET tarafından lisansları alınan güvenlik yazılımlarını sistemlerden kaldıramaz veya devre dışı bırakamaz.
b) İstemciden istemciye dosya paylaşım programlarını bilgisayarlara yüklemeleri ve kullanmaları yasaktır.
c) İşle ilgili olmayan veya telif hakları ile korunan dosyaları indirmeleri, depolamaları, çoğaltmaları ve paylaşıma açmaları yasaktır.
d) Lisansı temin edilmemiş yazılımlar kullanamaz.
e) Zararlı yazılımları sistemlere yükleyemez veya yüklemeye çalışamaz.
f) Sistemlerde açık servisleri ve güvenlik açıklarını tespit eden ağ trafiğini dinleyen programları yüklemeleri ve çalıştırmaları yasaktır. Tespit edilmesi halinde cezai işlemler başlatılır.

g) Üniversiteye ait bilgisayar ve çevre birimlerini, yan donanımlarını (mobil ürünler hariç) izinsiz olarak kullanım dışı bırakmaları, bunların yerlerini değiştirmeleri, kurum dışına çıkartmaları yasaktır.
h) BİDB'nin bilgisi dışında, kendilerine veya firmalara ait sistem ve donanımları yazılı izin veya sözleşme olmadan bilişim ve bilgi sistemlerine bağlayamaz.
i) Kullanımına yetkili olunmayan sunucu hizmetlerini çalıştıramaz ve sunucu sistemler üzerinde kişisel bilgisayar uygulamalarını kullanamaz.
j) Üniversitemize ait, halka açık olanlar dışındaki bilgileri kopyalamaları; internet üzerinde, haber gruplarında, posta listelerinde, forumlarda paylaşmaları yasaktır.
k) BİDB'den izin almadan çevirmeli ağ modemi, GPRS/Edge modemler, bluetooth ve kızılötesi iletişim cihazlarını sistemlere bağlayamaz.
l) Gizlilik dereceli bilgileri içeren yazılı veya elektronik belgelere yetkisiz şekilde erişmeye çalışmaları, erişmeleri, değiştirmeleri, bu belgeleri belirlenen alıcısı dışındaki kişi ve kurumlara teslim etmeleri, yetkisiz kişilerle paylaşmaları yasaktır.

İKİNCİ BÖLÜM

Politikalar

Madde 5- Elektronik Posta Politikası

5.1. Elektronik Posta Kullanımı

a) Elektronik posta kaynakları, BİDB tarafından belirlenerek onaylanmış kurallar çerçevesinde kullanılabilir.
b) Bilgi İşlem Daire Başkanlığı, uzun süre kullanılmayan hesapları kapatma hakkına sahiptir. 1 Yıl süreyle kullanılmayan hesaplar kapatılabilir ve ilgili kullanıcının dosyaları silinebilir.
c) Personel Daire Başkanlığından gelen bilgiye göre, Üniversitemizden ayrılan personelin elektronik posta hesabı kapatılır. Personel bu konuda geri bildirim yapılmayacağını kabul etmiş sayılır.
d) Üniversite elektronik posta adresini kullanan kullanıcı, işbu politika maddelerini ve Nuh Naci Yazgan Üniversitesi Bilgisayar, Ağ ve Bilişim Kaynakları Kullanım Politikası ile ilgili kanun ve yönetmeliklere de aykırı davranamaz.
e) Elektronik posta sisteminin işletilmesi, ilgili kanun ve yönetmeliklere göre yapılır.
f) Elektronik posta hesabı kullanıcısı, verilen hizmetlerden yararlanmaya başladığı andan itibaren bu politikada yer alan maddelere uyacağını kabul ve taahhüt eder. Aksi yönde bir tutum tespit edildiği takdirde elektronik posta kullanım hakkının sona erdirileceğini kabul etmiş sayılır. Kullanıcı kurallara uymadığı takdirde, bütün hukuki ve idari işlemlerden sorumludur.
g) BİDB, meydana gelebilecek yasal, idari ve teknolojik gelişmeler doğrultusunda bu kullanım politikasını değiştirebilir ve/veya güncelleyebilir. Kullanıcılar, bu politikaya uygun olarak bu hizmetten yararlanmak için bu politikaları gözden geçirmelidir.
h) Elektronik posta sistemini kullanan her kullanıcı, bu sistemi etkin ve güvenli kullanım bilgisine sahip olduğunu kabul eder.

5.2. Elektronik Posta Uygunsuz Kullanımı

a) Nuh Naci Yazgan Üniversitesi elektronik posta kaynakları yasa dışı şekilde kullanılamaz.
b) E-posta kullanımı kurumsal imaja zarar verecek, çıkarlarıyla çelişecek, kurumsal iş ve işlemleri engellemek için kullanılamaz. Nuh Naci Yazgan Üniversitesi Elektronik posta hesapları, uygunsuz ve kanun ve yönetmeliklere aykırı içeriği saklamak, bağlantı olarak eklemek, erişmek ve göndermek için kullanılamaz. Nuh Naci Yazgan Üniversitesi Elektronik posta hesapları; uygunsuz ve kanun ve yönetmeliklere aykırı içeriği saklamak, bağlantı olarak eklemek, erişmek ve göndermek için kullanılamaz.
c) Kullanıcılar e-posta hesaplarını, genel ahlak ilkelerine aykırı, alıcının istemi dışında ileti (SPAM ileti) göndermek amacıyla kullanılamaz. Çok sayıda kullanıcıya, izinsiz olarak reklam, tanıtım vb. amaçlı ileti gönderilemez.
d) Bilimsel, akademik ve idari iş süreçlerine uygun toplu duyurular, Bilgi İşlem Dairesi Başkanlığınca gönderilir. Toplu e-posta gönderilmesi Nuh Naci Yazgan Üniversitesi Genel Sekreterlik iznine bağlıdır. Bunun için ilgili birimlere müracaat edilmelidir.
e) Birimler arası ve birim içi e-posta gönderilmesi için bir toplu e-posta gönderim sistemi bulunmaktadır. Nuh Naci Yazgan Üniversitesi Genel Sekreterliği tarafından yetkilendirilen kişiler, kurum içinde yetkilendirildikleri birimlere toplu e-posta gönderebilirler.
f) Kullanıcı, e-posta hesabını ticari, siyasi, dini, etnik ve kar amaçlı olarak kullanamaz.
g) Kişinin/kurumun e-posta sistemin güvenliği için kullanıcılar, bilgi güvenliği farkındalığına sahip olmalıdır. Kaynağı bilinmeyen bir yerden gelen iletiler ve ekindeki dosyalar kesinlikle açılmamalı, virüs, truva atı vb. zararlı kodlar içerebileceğinden dolayı hemen silinmelidir.
h) Nuh Naci Yazgan Üniversitesi BİDB, kullanıcıların bilgi güvenliğine önem vermektedir. Kullanıcılardan, hiç bir şekilde parola (şifre), TC Kimlik numarası vb. kişisel bilgiler elektronik olarak istenilmemelidir. Buna benzer e-postalar kullanıcılar tarafından alınırsa, bu tür e-posta iletilerine cevap yazılmamalıdır. Bu tür epostaların kullanıcıları rahatsız etmemesi ve konu ile ilgili gerekli incelemenin ve gereğinin yapılabilmesi için Bilgi İşlem Daire Başkanlığı'na bu tür e-postalar bilgiislem@nny.edu.tr e-posta adresine göndermelidir.
i) Üniversite ile ilgili kritik bilgi varlıklarına ait verileri içeren bilgiler/belgeler/dokümanlar, elektronik posta ile gönderilemez.
j) Elektronik posta hesabında yer alan bilgilerin ve belgelerin yayın haklarından doğabilecek hukuki sorumluluklar tümüyle kullanıcıya aittir. Kullanıcı fikir ve sanat eserleri kanununa göre başkalarının fikir haklarını ihlal edici şekilde bilgiler/belgeler/dokümanlar dağıtımını yapamaz.

Madde 6- Parola Politikası

6.1. Parola Genel Kuralları

a) Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) en geç 6(altı) ayda bir değiştirilmelidir.
b) Kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) en geç 45(kırk beş) günde bir değiştirilmeli
c) Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.
d) Parolalar e- posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
e) Kullanıcı, parolasını başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda bilgilendirilmeli ve eğitilmelidir.

f) Kurum çalışanı olmayan kişiler için açılan kullanıcı hesapları da kolayca kırılamayacak güçlü bir parolaya sahip olmalıdır.
g) Bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.

6.2. Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır.

a) En az 6 haneli olmalıdır.
b) İçerisinde en az 1 tane harf bulunmalıdır. (a, b, C...)
c) İçerisinde en az 2 tane rakam bulunmalıdır. (1, 2, 3...)
d) İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,a,+,$,#,&,/,{,*,-,],=,...)
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 kelimeler içermemelidir. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)

6.3. Şifre koruma standartları ile ilgili kurallar aşağıda belirtilmiştir.

a) Bütün parolalar Kuruma 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.
c) Parola kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir.
d) Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilebilir.

Madde 7 – Antivürüs Politikası

7.1. Antivirus Politikası Genel Kurallar

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 çıkartılmalıdır.
c) Sistem yöneticileri, antivirüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
d) Kullanıcı hiç bir sebepten dolayı antivirüs yazılımını bilgisayarından kaldırmamalıdır.
e) Antivirüs güncellemeleri antivirüs sunucusu ile yapılmalıdır. Sunucular internete sürekli bağlı olup, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, otomatik olarak antivirüs sunucusu tarafından antivirüs güncellemeleri yapılmalıdır.

f) Etki alanına dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarları ağdan çıkartabilmelidir.
g) Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.
h) Üniversitenin ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.
i) Optik Media ve harici veri depolama cihazları antivirüs kontrolünden geçirilmelidir.
j) Kritik veriler ve sistem yapılandırmaları düzenli aralıklar ile yedeklenmeli ve bu yedekler farklı bir elektronik ortamda güvenli bir şekilde saklanmalıdır. Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı olmalıdır.

Madde 8- İnternet Erişim ve Kullanım Politikası

a) Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar(lar)ı üzerinden internete çıkmalıdır. Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.
b) Kurumun politikaları doğrultusunda içerik filtreleme sistemleri kullanılmalıdır.
c) İstenilmeyen siteler (pornografi, oyun, kumar, şiddet içeren vs.) yasaklanmalıdır.
d) Kurumun ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır.
e) Kurumun ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılmalıdır.
f) İnternete giden ve gelen bütün trafik virüslere karşı taranmalıdır.
g) Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri hayata geçirilmelidir.
h) Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemelidir.
i) İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilmemeli ve indirilmemelidir. Bu konuda gerekli önlemler alınmalıdır.
j) Üçüncü şahısların internet erişimleri için misafir ağı erişimi verilmelidir.

Madde 9- Sunucu Güvenlik Politikası

9.1. Sahip olma ve sorumluluklar ile ilgili kurallar

a) Üniversite'de bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel(ler) sorumludur.
b) Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel(ler) tarafından yapılmalıdır.
c) Sunuculara ait bilgilerin yer aldığı tablo oluşturulmalıdır. Bu tabloda, sunucuların isimleri, ipadresleri ve yeri, ana görevi ve üzerinde çalışan uygulamalar, işletim

sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personel(ler)in isimleri ve telefon numaraları bilgileri yer almalı ve bu tablo bir portal üzerinde bulundurulmalıdır.

d) Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.

9.2. Sunucu Güvenlik Politikası Genel kuralları

a) Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri BİDB talimatlarına göre yapılmalıdır.
b) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
c) Servislere erişimler, kaydedilerek ve erişim kontrol yöntemleri ile koruma sağlanmalıdır.
d) Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve antivirüs vb. koruma amaçlı yazılımlar sürekli güncellenmelidir. Antivirüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılmalıdır. Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, bir onay ve test mekanizmasından geçirilmeli, sonra uygulanmalıdır. Bu çalışmalar için yetkilendirilmiş bir personel olmalıdır.
e) Sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.
f) Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
g) Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.
h) Sunucular üzerinde lisanslı yazılımlar kurulmalıdır.
i) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

9.3. Sunucu Gözlemleme Kuralları

a) Kritik sistemlerde, uygulamalar kaydedilmeli ve kayıtlar aşağıdaki gibi saklanmalıdır.
b) Kayıtlara çevrimiçi olarak minimum 90 gün süreyle erişebilmelidir.
c) Günlük tape backuplar en az 1 ay saklanmalıdır.
d) Haftalık tape backuplar en az bir ay saklanmalıdır.
e) Aylık full backuplar en az 6 (altı) ay saklanmalıdır.
f) Kayıtlar sunucu üzerinde tutulmalarının yanı sıra ayrı bir sunucuda da saklanmalıdır.
g) Sunucu üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları, vb.) çalıştırılmamalıdır.
h) Kayıtlar sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.
i) Port tarama atakları düzenli olarak yapılmalıdır.
j) Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik yapılmalıdır.

k) Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.
l) Denetimler, BİDB tarafından yetkilendirilmiş kişilerce yönetilmeli ve belli aralıklarda yapılmalıdır.
m) Sunucuların bilgileri yetkilendirilmiş kişi tarafından bilgileri tutulmalı ve güncellenmelidir.

9.4. Sunucu İşletim Kuralları

a) Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, tavan ve taban güçlendirmeleri yapılmış ortamlarda bulundurulmalıdır.
b) Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.
c) Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve bilgisayar sistemine kayıt edilmelidir.

Madde 10- Ağ Cihazları Güvenlik Politikası

10.1. Ağ Cihazları Güvenlik Politikası

a) Ağ cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer almalıdır.
b) Yerel kullanıcı hesapları açılmamalıdır. Ağ cihazları kimlik tanımlama için LDAP, RADIUS veya TACAS+ protokollerinden birini kullanmalıdır.
c) Yönlendirici ve anahtarlardaki tam yetkili şifre olan ‘enable şifresi’ kodlanmış formda saklanmalıdır. Bu şifrenin tanımlanması kurumun içerisinden yapılmalıdır.
d) Kurumun standart olan SNMP community string’leri kullanılmalıdır. Bu bilgi sadece yetkilendirilmiş kişiler tarafından bilinmelidir.
e) İhtiyaç duyulduğu zaman erişim listeleri eklenmelidir.
f) Yönlendirici ve anahtarlar kurumun yönetim sisteminde olmalıdır.
g) Yazılım ve firmware güncellemeleri önce test ortamlarında denenmeli, sonra çalışma günlerinin dışında üretim ortamına taşınmalıdır.
h) Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.
i) Bilgisayar ağında bulunan kabinetler, aktif cihazlar, ağ kabloları (UTP ve fiber optik aktarma kabloları), cihazların portları etiketlenmelidir.
j) 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, bu politikaya uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptırım olabilir.”

10.2. Ağ Yönetim Politikası

a) Ağ cihazları yönetim sorumluluğu, sunucu ve istemcilerin yönetiminden ayrılmalıdır.

b) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılmalı ve güncellemeler uygulanmalıdır.
c) Erişimine izin verilen ağlar, ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmeli ve yetkisiz erişimle ilgili tedbirler alınmalıdır.
d) Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanmalıdır.
e) Sınırsız ağ dolaşımı engellenmelidir.
f) Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaçlara göre serbest bırakılmalıdır.
g) Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınmalıdır.
h) İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmalı ve kayıtlar tutulmalıdır.
i) Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır. Kurum kullanıcılarının bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılmalı ve ağlar arasında geçiş güvenlik sunucuları (firewall) üzerinden sağlanmalıdır.
j) Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.
k) Bilgisayar ağına bağlı bütün makinelerde kurulum ve yapılandırma parametreleri, Kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.
l) Sistem tasarımı ve geliştirilmesi yapılırken Kurum tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanılmalıdır.
m) İnternet trafiği, İnternet Erişim ve Kullanım Politikası ve ilgili standartlarda anlatıldığı şekilde izlenebilmelidir.
n) Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı şekilde saklanmalıdır.
o) Ağ cihazları görevler dışında başka bir amaç için kullanılmamalıdır.
p) Ağ cihazları yapılandırılması Sistem Yöneticisi tarafından veya Sistem Yöneticisinin denetiminde yapılmalı ve değiştirilmelidir.
q) Ağ dokümantasyonu hazırlanmalı ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanmalıdır.

Madde 11 - Uzaktan Erişim Politikası

a) Internet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. 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 denetlenmelidir.
c) Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.
d) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

e) Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılmalıdır.
f) Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve antivirüs yazılımı güncellemeler yapılmış olmalıdır.
g) Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

11.1. Uzaktan Erişim Yönetimi

a) Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.
b) İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamalıdır. VPN teknolojileri İpSec, SSL, VPDN, PPTP, L2TP vs. protokollerinden birini içermelidir. Uzaktan erişim güvenliği sıkı şekilde denetlenmelidir.
c) Kontrol tek yönlü şifreleme (one-time password authentication, örnek; SMS,E-mail,Token Device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmelidir. Daha fazlası için parola politikasına bakınız.
d) Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.
e) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.
f) Mobile VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile
yapılmalıdır.
g) Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.
h) Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.
i) Uzak erişimde yapılan tüm network hareketleri loglanmalıdır.
j) Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.
k) Uzak erişim verilecek olan kullanıcılara sözleşmesine göre günlük saatlik izinler verilmelidir.
l) Sınırsız izin verilmekten kaçınılmalıdır.
m) VPN ile erişecek olan kullanıcı VPN Erişim formunu doldurmak zorundadır.
n) Uzak erişim bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmelidir.

11.2. Acil Erişim Yetkilendirme Yönetimi

a) Acil erişim yetkilendirme gerektiren durumlarda uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.

b) Kurum bünyesindeki bütün dahili sunucuların, ağ güvenliği ve şebeke cihazları ile veri tabanı yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur.
c) Kurum bünyesindeki yazılım ve veri güvenliğini sağlarken yetkilendirilmiş sistem yöneticisi Güvenliği sağlamaktan sorumlu Ağ ve Sistem Güvenliği birimi ile birlikte uyumlu çalışarak sağlamak zorundadır.
d) Sunuculara ve cihazlara acil erişim yetkilendirilmesi gereken durumlarda; kurum içi kullanıcı, yetkilendirilmiş sistem yöneticisine başvurarak sistem üzerinde yetki istemelidir.
e) Veri tabanına acil erişim yetkilendirilmesi gereken durumda; kurum içi kullanıcı için erişim yetkilendirmesinde veri tabanı güvenlik politikası maddelerine bakılır.
f) Acil erişim yetkisi gereken durumlarda kurum dışı kullanıcılar için resmi taahhütname gelmeden uzak erişim yetkisi verme isteği acil erişim gereken birim yetkilisi tarafından verilmelidir.
g) Başka birimlerden alınması gereken erişim yetkisinin sorumluluğu, isteği yapan birimin yetkilendirilmiş yöneticisinin sorumluluğundadır.
h) Sistem üzerinde verilecek erişim yetkisi ve bunun doğuracağı sorumluluk sunucu/cihaz üzerinde yetki veren yetkilendirilmiş sistem yöneticisinindir.
i) Kritik sistemlerde veri güvenliğini sağlamak için sistem yöneticisi gerekli güvenlik tedbirlerini almalıdır. Güvenliği sağlamak için gereken durumlarda başka birimler ile birlikte çalışmalıdır.
j) Veri tabanlarında bulunan bir veriye acil olarak erişilmesi gerektiğinde, verinin bulunduğu
tablonun sahibinden eposta ortamında izin alındıktan sonra erişim izni veri tabanı birimi tarafından verilmelidir.

Madde 12 - Kablosuz İletişim Politikası

a) Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınmalıdır.
b) Bütün kablosuz erişim cihazları Bilgi İşlem Güvenlik Birimi tarafından onaylanmış olmalı ve Bilgi İşlemin belirlediği güvenlik ayarlarını kullanmalıdır.
c) Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.
d) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılmalıdır. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır.
e) Erişim cihazlarındaki firmwareler düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlamaktadır.
f) Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.
g) Varsayılan SSID isimleri kullanılmamalıdır. SSID ayarı bilgisi içerisinde kurumla ilgili bilgi olmamalıdır, mesela kurum ismi, ilgili bölüm, çalışanın ismi vb.

h) Radyo dalgalarının binanın dışına taşmamasına özen gösterilmelidir. Bunun için çift yönlü antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanmalıdır.
i) Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Kurum kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanmalı ve Kurum kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenmelidir.
j) Erişim Cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dâhil olmalıdırlar.
k) Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından Kurum'un tüm internet bant genişliğinin tüketilmesi engellenmelidir.
l) Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlı olmalıdır.
m) Kullanıcı bilgisayarlarında kişisel antivirüs ve güvenlik duvarı yazılımları yüklü olmalıdır.
n) Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

Madde 13 - Yazılım Güvenliği

a) Kurum içerisinde kullanılan tüm bilgisayarların zararlı yazılımlara karşı en güncel anti virüs yazılımına sahip olmalıdır.
b) Bilgisayarlarda kullanılan anti virüs yazılımları düzenli olarak güncellenmelidir.
c) Bilgisayarların üzerinde kullanılan işletim sistemleri düzenli olarak güncelleştirilmelidir.
d) Bilgisayarlar üzerinde korsan yazılımlar bulundurulmamalıdır.
e) Kurum için hazırlanacak uygulamalar güvenlik zafiyetlerini en aza indirmek için güvenli yazılım yaşam döngüsüne uygun olarak tasarlanmalıdır.
f) Geliştirilen yazılımlar gizlilik, bütünlük ve erişebilirlik şartlarına uygun olmalıdır.
g) Yazılım geliştirme sürecinde, giriş doğrulama, yetkilendirme, kimlik doğrulama, konfigürasyon yönetimi, hassas bilgi, kriptografi, parametre manipülasyonu, hata yönetimi ve kayıt tutma ve denetimi kriterleri dikkate alınmalıdır.
h) Yazılım geliştirme süreci boyunca, gerekli bütün testler eksiksiz şekilde yapılmalıdır.
i) Kurum için geliştirilen uygulamalar ve satın alınan yazılımlar, güvenlik zafiyetlerine neden olmamak için en son stabil yamalara ve güncelleştirmelere sahip olmalıdır.
j) Uygulamalar geliştirilme süreçlerinde gerçek ortamda uygulanmadan önce test sunucularında test edilmelidir. Uygulamalar gerçek ortamda kurumun uygun bulduğu mesai saatleri dışında bir zaman diliminde devreye alınmalıdır.
k) Kurum için geliştirilen uygulamalar, uluslararası kabul görmüş standartlara bağlı dokümante edilmelidir. Uygulama için yazılmış olan dokümanlar uygulama ile beraber kuruma teslim edilmelidir.

Madde 14 - Donanım Güvenliği

a) Kuruma ait sistemler ve sunucular dışarıdan gelebilecek saldırılara karşı, güncel teknolojilere sahip donanımsal firewall cihazları ile korunmalıdır.

b) Kurum çalışanlarının internete çıkışlarının kontrol edilerek, zararlı ve kurum politikasına uymayan sitelere erişimlerinin engellenmesi için proxy cihazları ile korunmalıdır.
c) Kuruma ait uygulamaların güvenli bir şekilde çalışması ve uygulamalara gelebilecek saldırıların engellenmesi için Web Application Firewall (Web Uygulama Güvenlik Duvarı) ile korunmalıdır.
d) Kurum ile dış dünya arasında ki yazışmalar bir eposta güvenlik cihazı ile kontrol edilmelidir.
e) SPAM, virüs, kurum politikalarına uygun olmayan içerikler engellenmelidir.
f) Kurumda ki güvenlik cihazları sürekliliğin sağlanması için cluster (yedekli yapıda) bulunmalıdır.
g) Kurumda kullanılan güvenlik cihazlarının loglarının düzenli olarak alınması ve encrypt (şifreli) olarak saklanması gerekmektedir.
h) Kurumda kullanılan bütün güvenlik cihazlarının konfigürasyon yedekleri periyodik olarak alınmalı, doğru şekilde etiketlenerek saklanmalıdır.
i) Kurumda kullanılan bütün sistem ve güvenlik donanımları, kurumun ihtiyaçlarına bağlı olarak sadece izin verilen erişimlere göre konfigüre edilmelidir.

Madde 14 - Yazılım Geliştirme Politikası

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.
d) Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.
e) Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.
f) Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.
g) 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.
h) Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.
i) Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.
j) Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.
k) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.
l) Yazılımlar sınıflandırılmalı / etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

Madde 15 - Veritabanı Güvenlik Politikası

a) Veritabanı sistemleri envanteri dokümante edilmeli ve bu envanterden sorumlu personel tanımlanmalıdır.

b) Veritabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.
c) Veritabanı sistem kayıtları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.
d) Veritabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir.
e) Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.
f) Yedekleme planları dokümante edilmelidir.
g) Manyetik kartuş, DVD veya CD ortamlarında tutulan log kayıtları en az 2 (iki) yıl süre ile güvenli ortamlarda saklanmalıdır.
h) Veritabanı erişim politikaları "Kimlik Doğrulama ve Yetkilendirme" politikaları çerçevesinde oluşturulmalıdır.
i) Hatadan arındırma, bilgileri yedekten dönme kuralları "Acil Durum Yönetimi" politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.
j) Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
k) Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.
l) Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.
m) Bilgi saklama medyaları kurum dışına izinsiz çıkartılmamalıdır.
n) Sistem dokümantasyonu güvenli şekilde saklanmalıdır.
o) İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.
p) 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.
q) Uygulama sunucularından veritabanına rlogin vb. şekilde erişememelidir.
r) Veritabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak kurumun kasasında saklanmalı ve gereksiz yere açılmamalıdır. Zarfın açılması durumunda firma yetkilileri de bilgilendirilmelidir.
s) Arayüzden gelen kullanıcılar bir tabloda saklanmalı, bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmalıdır.
t) Veritabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak bağlanılmalıdır. Root veya admin şifresi tanımlı kişi/kişilerde olmalıdır.
u) Bağlanacak kişilerin kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.
v) Bütün kullanıcıların yaptıkları işlemler kaydedilmelidir.
w) Veritabanı yöneticiliği yetkisi sadece bir kullanıcıda olmalıdır.
x) Veritabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.
y) Veritabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar tesis edilmelidir.
z) Veritabanı sunucularına ancak yetkili kullanıcılar erişmelidir.

aa) Veritabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıclar bağlanıp sorgu yapmamalıdır.
bb) Veritabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir. (Ağ trafiğini dinleyen casus yazılımların verilere ulaşamaması için)
cc) Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için Şifreleme Politikasına bakılmalıdır.
dd) Veritabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için de geçerlidir.

Madde 16 - Erişim Yönetimi ve Erişim Kayıtlarının Tutulması Politikası

Veri tabanlarına erişen kullanıcıların yapmış oldukları işlemler loglanmalı, gerektiğinde erişim yetkilisinin kayıt silme logları da listelenebilir olmalıdır.

16.1. Erişim Yönetimi

Kurumun erişim sağlanacak sunucularına admin/root yetkili yönetici kullanıcılar, sudo ve runas yetkili kısıtlı yönetici kullanıcılar ve dış dünyadan erişen, uygulamayı kullanan kullanıcılardan oluşmaktadır.

a) Sunuculara erişim için IP/SEC ya da SSL VPN kullanılmalıdır. Mümkünse kullanıcıların erişimi için SSL ve VPN tercih edilmelidir. Güvenlik Birimi tarafından sağlanmalıdır.
b) Sunuculara kullanıcı erişimi için SSH, RDP gibi protokollerle sunucu yönetimi için belirli portlar erişim verilmelidir.
c) Sunucuların kendi aralarında servis ve yönetimleri için belirli portlarla erişim sağlanması gerekmektedir.
d) Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir. Parola yönetimi bilgi güvenliği politikası parola yönetim politikaları ile yürütülmelidir.
e) Kullanıcıların sunucu yönetim için sağlanan erişimde merkezi kullanıcı yönetimi (MS AD, LDAP, ssh-key) ile yapılmalıdır.
f) Kullanıcıların sunucu yönetim için sağlanan erişimde sudo, runas gibi erişim kısıtlı erişim yetkileri tanımlanmalıdır.
g) Dış dünyadan sunucular üzerindeki servislere erişim için 80, 443, 7001, 8080, 8443 gibi servis portları da özel durumlarda verilmelidir. Güvenlik Birimi tarafından bu işlem sağlanmalıdır.
h) Sunucu servislerinin yönetim işlemlerinde yetkili kullanıcı bilgileri, sistem gurubuna teslim edilmelidir. Sistem birimi nezaretinde ve tarafından yürütülmelidir.
i) Sunucu servislerinin yönetim işlemleri merkezi kullanıcı yönetimi ve kısıtlı erişim yetkileriyle kullanıcılara sağlanmalıdır.
j) Kurumun yedekleme sistemlerine sadece memur ya da danışman yetkili kişi erişim yapmaktadır.
k) Firmaların yapacakları tüm işlemler sistem birimi nezaretinde yürütülmelidir.

16.2. Kayıt Tutulması (Log tutulması)

a) Kurumun güvenlik cihazlarına ait loglar güvenlik birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.
b) Kurumun veri tabanlarına ait loglar veri tabanları birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.
c) Kurumun network cihazlarına ait loglar network birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.
d) Tüm sunuculara ve servislere sağlanan tüm yönetici erişimleri uzak ve merkezi bir kayıt sunucusuna gönderilmelidir.
e) Merkezi kayıt sunucusu üzerinde yapılan analizler sonucunda başarısız erişimler raporlanmalıdır.
f) Merkezi kayıt sunucusu üzerinde alınan başarısız erişim istekleri uyarı olarak yetkili Birimlere gönderilmelidir.
g) Merkezi kayıt sunucusu üzerindeki başarılı girişler de istatiksel veriler halinde raporlanabilmelidir.
h) Merkezi kayıt sunucusu üzerindeki kayıt verileri belirli tarih aralığında tutulmalı ve istenildiğinde raporlanabilir olmalıdır.
i) Merkezi kayıt sunucusu kayıtlar üzerinde yaptığı analizler doğrultusunda saldırı ve normal olmayan durumları tespit edip, uyarı gönderebilmelidir.

Madde 17 - Kimlik Doğrulama ve Yetkilendirme Politikası

a) Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecek ve dokümante edilecektir.
b) Kurum sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacak ve dokümante edilecektir.
c) Kurum 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 belirlenmeli, dokümante edilmeli ve denetim altında tutulmalıdır.
d) Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve bu gereksinimler gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.
e) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.
f) Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulmalı, tekrarlanan başarısız erişim istekleri/girişimleri incelenmelidir.
g) Kullanıcılara erişim hakları yazılı olarak beyan edilmelidir.
h) Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

i) Sistemler üzerindeki tüm roller, rollere sahip kullanıcılar ve rollerin sistem kaynakları üzerindeki yetkileri uygun araçlar kullanılarak belirli aralıklarla listelenmelidir. Bu listeler yetki seviyeleri ile karşılaştırılmalıdır. Eğer uyumsuzluk varsa dokümanlar ve yetkiler düzeltilerek uyumlu hale getirilmelidir.

Madde 18 - Bilgi Kaynakları Atık ve İmha Politikası

a) Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.
b) Yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.
c) Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmi Gazete 'de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleşmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.
d) İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.
e) Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.
f) Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.
g) Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
h) Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.
i) Hacimsel küçültme işlemi için parçalanmalıdır.
j) Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.
k) Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

Madde 19 - Veri Yedekleme ve İş Sürekliliği Politikası

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 yedeklenmelidir.
b) Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde veya offline olarak manyetik kartuş, DVD veya CD ortamında yedekleri alınmalıdır.

c) Taşınabilir ortamlar (manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından faklı odalarda veya binalarda güvenli bir şekilde saklanmalıdır. Veriler offline ortamlarda en az 1 (bir) yıl süreyle saklanmalıdır.
d) Kurumsal kritik verilerin saklandığı veya sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.
e) Düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamaların çalıştığı ve yedeği alınacak dizin, dosya bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.
f) Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
g) Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.
h) Yedek ünite üzerinde gereksiz yer tutmamak amacıyla, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dâhil edilmemelidir.
i) Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.
j) Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenmelidir.
k) Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir.
l) Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.
m) Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
n) Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dâhilinde tamamlanması gerekmektedir.
o) Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.
p) Yedekleme Standardı ile doğru ve eksiksiz yedek kayıt kopyaları bir felaket anında etkilenmeyecek bir ortamda bulundurulmalıdır.
q) 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 belirlenmelidir. Yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerliği periyodik olarak gözden geçirilmelidir.

Madde 20 - Son Kullanıcı Güvenliği Politikası

a) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.
b) Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilmeli ve teyit alınmalıdır.
c) Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin

edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorulması sağlanmalıdır.

d) Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.
e) Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.
f) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.
g) İş tanımı değişen veya Kurumdan ayrılan kullanıcıların erişim hakları kaldırılmalıdır.
h) Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
i) Kurum bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim lanlamaları periyodik olarak yapılmalı, bütçe ayrılmalı, eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.
j) 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.
k) Çalışanlar, kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler, görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe alınan elemanlar için de bu eğitim, uyum süreci sırasında verilmelidir.
l) Çalışanların güvenlik ile ilgili aktiviteleri izlenmelidir.
m) Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların
iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır.

Madde 21 - Kişisel Verilerin Korunması ve İşlenmesi Politikası

Üniversite kişisel verilerin korunması ve işlenmesi için gerekli tedbirleri ve uygulanan süreci politika ile somut bir şekilde belirler.

21.1. Kişisel Verilerin Güvenliğinin Sağlanması

Üniversite, KVKK'nın 12 inci maddesinin 1inci fıkrasında öngörülen;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
c) Kişisel verilerin muhafazasını sağlamak,

için gerekli her türlü teknik ve idari tedbirleri alır.

Üniversitenin kişisel verilerin güvenliğini sağlamak için uyguladığı tedbirler alt maddelerde detaylandırılmıştır.

21.2.Teknik Tedbirler

a) BİDB, kurulan sistemler için gerekli iç kontrolleri yapar.
b) Kurulan sistemler kapsamında risk analizi, veri sınıflandırması, bilgi güvenliği risk değerlendirmesi ve iş etki analizinin gerçekleştirilmesi süreçlerini işletir.
c) Bu süreçler doğrultusunda teknolojideki gelişmelere uygun teknik önlemleri alır.
d) Gelişen teknolojiye uygun altyapı yatırımları yapar.
   - Virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımların kurulmasını sağlar.
   - Sistemlerinin güncel ve bilinen açıklıklara karşı gerekli güvenlik önlemlerinin alınmış versiyonlarını kullanır.
   - Üniversite birimlerinde çalışanların kişisel verilere erişimi yetkilerinin kontrol altında tutulmasını sağlar.
   - Üniversitede işlenmekte olan kişisel verilerin saklandığı fiziki alanlar, çalınmaya ve kaybolmaya karşı gerekli fiziksel güvenlik önlemleri alınarak muhafaza edilir. Aynı şekilde kişisel verilerin yer aldığı ortamlar dış risklere (yangın, sel, deprem vb.) karşı gerekli uygun yöntemler belirlenerek koruma altına alınır. Bu ortamlara giriş çıkışlar kayıt altına alınarak izlenir.
   - Kişisel veri barındıran sunucular Üniversite sistem odasında muhafaza edilir.
   - Sistem odasının fiziki güvenlik önlemleri alınır.
   - Kişisel veri barındıran sistem, uygulama, veri tabanı vb. alanlara erişim için kullanılmakta olan şifreler, karmaşık bir algoritma ile üretilir ve sistemler bu şekilde kullanılmaya teşvik edilir.
   - İş birim bazlı belirlenen hukuksal uyum gerekliliklerine uygun olarak erişim ve yetkilendirme tanımlarını yapar.
   - Erişimlerin yetkilendirmelere uygunluğunu kontrol eder.
   - Risk teşkil eden noktalar tespit edilerek gerekli teknik tedbirler alınır.
   - Kişisel verilerin güvenliğinin sürdürülebilmesi için teknik tedbirleri sürekli işleyen bir model ile kurum kültürünün bir parçası olması için farkındalığı yaygınlaştırır.
   - Kamera kayıtlarına erişimde kullanıcı yetkilendirilmesi yapılır ve veriler güvenli ortamda saklanır.

Madde 22 - Bakım Politikası

a) Kurum sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için gerekli anlaşmalar için yıllık bütçe ayrılmalıdır.
b) Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.
c) Sistem üzerinde yapılacak değişiklikler ile ilgili olarak "Değişim Yönetimi Politikası" ve ilişkili standartlar uygulanmalıdır.
d) Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenmelidir.
e) Sistem bakımlarının ilgili politika ve standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik uygunluk ve güvenlik testleri yapılmalıdır.

f) Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda "Nuh Naci Yazgan Üniversitesi Bilgi Güvenlik Politikaları" uyarınca hareket edilmelidir.

Madde 23 - Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri

Kurum içerisinde bilgi güvenliği teknik ve farkındalık eğitimleri için yıllık bir plan yapılmalıdır. b) Yıllık planlar çerçevesinde bilgi güvenliği teknik ve farkındalık eğitimleri gerçekleştirilmelidir. c) Sunulan bilgi güvenliği teknik ve farkındalık eğitimleri katılım öncesi ve sonrası çeşitli ölçme teknikleriyle ölçülmeli ve eğitim etkililiği hususunda değerlendirme yapılmalıdır.

Kurumların teknik işlerinde (Bilişim faaliyetleri), uygulama geliştirme, sistem güvenliği kapsamında hizmet veren personellerin kişisel gelişimlerinin devamlılığı konusunda eğitimler düzenlenmelidir.

Eğitime katılım formları muhafaza edilmelidir. Eğitim faaliyetleri işlemlerinin, kurum içerisinde nasıl yürütülmesi gerektiği hususunda bir prosedür geliştirilmelidir.

ÜÇÜNCÜ BÖLÜM
Diğer Hükümler

Uygulama ve Yaptırım

Madde 24 - Üniversitede BGYS politika ve prosedürlerine uyulmadığının tespit edilmesi hâlinde, bu ihlalden sorumlu olan personel, öğrenci ya da 3. taraf için geçerli olan mevzuat ve sözleşmelerde belirlenen yaptırımlar uygulanır. Yönerge esaslarının ihlali, Rektörlüğün ilgili ve yetkili kanalları yoluyla işleme konulur.