

	NUH NACİ YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

İçindekiler

1. Genel Hükümler.....	3
2. Uygulamalar	3
3. Politikalar	5
3.1. Elektronik Posta Politikası	5
3.1.1. Elektronik Posta Kullanımı.....	5
3.1.2. Elektronik Posta Uygunsuz Kullanımı	6
3.2. Parola Politikası	7
3.2.1. Parola Genel Kuralları.....	7
3.2.2. Güçlü Parola Kuralları	7
3.2.3. Parola Koruma Kuralları.....	7
3.3. Antivürüs Politikası	7
3.3.1. Antivirus Politikası Genel Kurallar	7
3.4. İnternet Erişim ve Kullanım Politikası.....	8
3.5. Sunucu Güvenlik Politikası.....	9
3.5.1. Sahip Olma ve Sorumluluklar İle İlgili Kurallar.....	9
3.5.2. Sunucu Güvenlik Politikası Genel kuralları	9
3.5.3. Sunucu Gözleme Kuralları	9
3.5.4. Sunucu İşletim Kuralları.....	10
3.6.1. Ağ Yönetim Politikası	11
3.7. Uzaktan Erişim Politikası.....	11
3.7.1. Uzaktan Erişim Yönetimi.....	12
3.7.2. Acil Erişim Yetkilendirme Yönetimi.....	13
3.8. Kablosuz İletişim Politikası.....	13
3.9. Yazılım Güvenliği Politikası	14
3.10. Yazılım Geliştirme Politikası.....	15
3.11. Veritabanı Güvenlik Politikası.....	15
3.12. Donanım Güvenliği Politikası.....	17
3.13. Erişim Yönetimi ve Erişim Kayıtlarının Tutulması Politikası.....	17
3.13.1. Erişim Yönetimi.....	17



**NUH NACİ YAZGAN
ÜNİVERSİTESİ**
**BİLGİ GÜVENLİĞİ YÖNETİM
SİSTEMLERİ POLİTİKASI**

Doküman Kodu	BİDB-BGYS-02
Yürürlük Tarihi	21/11/2019
Revizyon Tarihi/No.	01/12/2021/01

3.13.2. Kayıt Tutulması (Log tutulması).....	18
3.14. Kimlik Doğrulama ve Yetkilendirme Politikası	18
3.15. Bilgi Kaynakları Atık ve İmha Politikası	19
3.16. Veri Yedekleme ve İş Sürekliliği Politikası.....	20
3.17. Son Kullanıcı Güvenliği Politikası	21
3.18. Kişisel Verilerin Korunması ve İşlenmesi Politikası.....	22
3.18.1. Kişisel Verilerin Güvenliğinin Sağlanması	22
3.18.2. Teknik Tedbirler.....	22
3.19. Bakım Politikası.....	23
3.20. Bilgi Güvenliği Teknik ve Farkındalık Eğitim Politikası	23
3.21. Basılı Çıktı ve Dağıtım Politikası	23
3.22. Bilgi Sınıflandırma Politikası.....	24
3.23. Bilgi ve Yazılım Alışverişi Politikası.....	24
3.24. Değişim Yönetimi Politikası	25
3.25. Fiziksel Güvenlik Politikası	26
3.26. Kabul Edilebilir Kullanım Politikası	26
3.27. Kriptografik Kontroller Politikası	27
3.28. Temiz Masa Temiz Ekran Politikası.....	28
3.29. Varlıklara Yönelik Sorumluluk Politikası	28
3.30. Ziyaretçi Kabul Politikası.....	28
3.31. Taşınabilir Cihaz Politikası.....	29
4. Diğer Hükümler	29
4.1. Uygulama ve Yaptırım	29

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

Misyon

Eğitim-öğretim, araştırma-geliştirme faaliyetleri ile idari ve yönetsel işlevler için gelişen bilgi teknolojilerini kullanıma sunmak, Üniversitemiz akademik ve idari personel ile öğrencilerin gereksinim duyacağı bilişim hizmetleri ve servislerinin karşılanmasında ihtiyaç duyulan yazımsal 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.

1. Genel Hükümler

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

1.2. 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.

1.3. 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.

2. Uygulamalar

2.1. 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;

- 1) Bilgi Güvenliği Politikaları kurumun güvenilirliğini ve itibarını korumayı sağlar.
- 2) Bilgi Güvenliği Politikaları kurumun ve paydaşlarının bilgi varlıklarına güvenli bir şekilde erişimini sağlar.
- 3) Bilgi Güvenliği Politikası kurumun ve paydaşlarının bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi sağlar.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- 4) Bilgi güvenliğinin ihlali durumunda gerekli görülen yaptırımları uygular.
- 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.
- 6) İş/Hizmet sürekliliğine karşı bilgi güvenliği tehditlerinin etkisini azaltır ve işin sürekliliği ile sürdürülebilirliğini sağlar.
- 7) Çeşitli kontrollerle bilgi güvenliği seviyesini korumayı ve iyileştirmeyi taahhüt eder.
- 8) NNYÜNET kullanıcıları bilgi güvenliği politikalarına, talimat ve prosedürlerine uymakla yükümlüdür.
- 9) NNYÜNET kullanıcılarını içeriden veya dışarıdan gelebilecek tehditlere karşı korumak, üretilen veya kullanılan bilgilerin gizliliğini güvence altına alarak NNYÜNET'in imajını korumakla yükümlüdür.
- 10) Üçüncü taraflarla yapılan sözleşmelerde güvenlik prosedürleri belirlenir.
- 11) Bilgi Güvenliği prosedürlerini yerine getirerek personelin bilgi güvenliği farkındalıklarını artırır.
- 12) Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlar.
- 13) NNYÜNET kullanıcıları, kritiklik düzeylerine göre işlediği bilgiyi yedekler.
- 14) NNYÜNET kullanıcıları, bilgi güvenliği ihlal olaylarını bilgi güvenliği yetkilisine bildirmeli, raporlamalı ve bu ihlalleri engelleyecek önlemleri almalıdır.
- 15) NNYÜNET bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.
- 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.
- 17) Bilgi güvenliği politikalarının yürütülmesi Bilgi İşlem Dairesi Başkanlığı (BİDB) tarafından yerine getirilir.
- 18) NNYÜNET kullanıcıları bilgi güvenliği kapsamında aşağıda belirtilen kurallara uymakla yükümlüdür:
 - a) NNYÜNET 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 paylaşımına 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.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- 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.

3. Politikalar

3.1. Elektronik Posta Politikası

3.1.1. Elektronik Posta Kullanımı

- a) Elektronik posta kaynakları, BİDB tarafından belirlenerek onaylanmış kurallar çerçevesinde kullanılabilir.
- b) BİDB, 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.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

3.1.2. 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, BİDB tarafından gönderilir. Toplu e-posta gönderilmesi Nuh Naci Yazgan Üniversitesi Rektörlüğü 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 Rektörlüğü 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) BİDB, kullanıcıların bilgi güvenliğine önem vermektedir. Kullanıcılardan, hiçbir şekilde parola (şifre), TC Kimlik numarası vb. kişisel bilgiler elektronik olarak istenilmemelidir. Buna benzer e-postalar kullanıcılar tarafından alınır, bu tür e-posta iletilerine cevap yazılmamalıdır. Bu tür e-postaların kullanıcıları rahatsız etmemesi ve konu ile ilgili gerekli incelemenin ve gereğinin yapılabilmesi için BİDB'ye bu tür e-postalar bilgiislem@nny.edu.tr e-posta adresine gönderilmelidir.
- 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.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

3.2. Parola Politikası

3.2.1. Parola Genel Kuralları

- Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) en geç 6(altı) ayda bir değiştirilmelidir.
- Kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) en geç 45(kırk beş) günde bir değiştirilmeli
- Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.
- Parolalar e- posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Kullanıcı, parolasını başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda bilgilendirilmeli ve eğitilmelidir.
- Kurum çalışanı olmayan kişiler için açılan kullanıcı hesapları da kolayca kırılmayacak güçlü bir parolaya sahip olmalıdır.
- Bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.

3.2.2. Güçlü Parola Kuralları

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

3.2.3. Parola Koruma Kuralları

- Bütün parolalar Kuruma ait gizli bilgiler olarak düşünülmesi ve kullanıcı, parolalarını hiç kimseye paylaşmamalıdır.
- Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki “parola hatırlama” seçeneği kullanılmamalıdır.
- Parola kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir.
- Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilebilir.

3.3. Antivürüs Politikası

3.3.1. Antivirus Politikası Genel Kurallar

- Üniversitenin tüm istemcileri ve sunucuları antivirüs yazılımına sahip olmalıdır. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak antivirüs yazılımı yüklenmeyebilir.
- İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalıdır.

	NUH NACİ YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- c) Sistem yöneticileri, antivirüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
- d) Kullanıcı hiçbir 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.
- k) Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı olmalıdır.

3.4. İnternet Erişim ve Kullanım Politikası

- a) Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar/duvarları üzerinden internete çıkmalıdır. Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşılabileceği 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 güvenlik yazılımı 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.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

3.5. Sunucu Güvenlik Politikası

3.5.1. Sahip Olma ve Sorumluluklar İle İlgili Kurallar

- Üniversite’de bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel/personeller sorumludur.
- Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel/personeller tarafından yapılmalıdır.
- Sunuculara ait bilgilerin yer aldığı tablo oluşturulmalıdır. 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 sorumlu personel/personeller’in isimleri ve telefon numaraları bilgileri yer almalı ve bu tablo bir portal üzerinde bulundurulmalıdır.
- Tüm bilgiler, sistem yöneticisinin belirlediği kişi/kişiler tarafından güncel tutulmalıdır.

3.5.2. Sunucu Güvenlik Politikası Genel kuralları

- Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri BİDB talimatlarına göre yapılmalıdır.
- Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
- Servislere erişimler, kaydedilerek ve erişim kontrol yöntemleri ile koruma sağlanmalıdır.
- 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.
- Sistem yöneticileri ‘administrator’ ve ‘root’ gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.
- Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
- Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN’larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.
- Sunucular üzerinde lisanslı yazılımlar kurulmalıdır.
- Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

3.5.3. Sunucu Gözleme Kuralları

- Kritik sistemlerde, uygulamalar kaydedilmeli ve kayıtlar aşağıdaki gibi saklanmalıdır.
- Kayıtlara çevrimiçi olarak minimum 90 gün süreyle erişebilmelidir.
- Günlük yedekler en az bir ay saklanmalıdır.
- Haftalık yedekler en az bir ay saklanmalıdır.
- Aylık yedekler en az 6 (altı) ay saklanmalıdır.

	NUH NACİ YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- 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.

3.5.4. 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.

3.6. 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.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

3.6.1. Ağ Yönetim Politikası

- Ağ cihazları yönetim sorumluluğu, sunucu ve istemcilerin yönetiminden ayrılmalıdır.
- Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılmalı ve güncellemeler uygulanmalıdır.
- Erişimine izin verilen ağlar, ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmeli ve yetkisiz erişimle ilgili tedbirler alınmalıdır.
- Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanmalıdır.
- Sınırsız ağ dolaşımı engellenmelidir.
- Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaçlara göre serbest bırakılmalıdır.
- Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınmalıdır.
- İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmalı ve kayıtlar tutulmalıdır.
- 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.
- Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.
- Bilgisayar ağına bağlı bütün makinelerde kurulum ve yapılandırma parametreleri, Kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.
- Sistem tasarımı ve geliştirilmesi yapılırken Kurum tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanılmalıdır.
- İnternet trafiği, İnternet Erişim ve Kullanım Politikası ve ilgili standartlarda anlatıldığı şekilde izlenebilmelidir.
- Bilgisayar ağındaki adresler, ağına ait yapılandırma ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı şekilde saklanmalıdır.
- Ağ cihazları görevler dışında başka bir amaç için kullanılmamalıdır.
- Ağ cihazları yapılandırılması Sistem Yöneticisi tarafından veya Sistem Yöneticisinin denetiminde yapılmalı ve değiştirilmelidir.
- Ağ dokümantasyonu hazırlanmalı ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanmalıdır.

3.7. Uzaktan Erişim Politikası

- 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 sağlamaktadır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. Protokollerinden birini içermelidir.
- Uzaktan erişim güvenliği denetlenmelidir.
- Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

	NUH NACİ YAZGAN ÜNİVERSİTESİ	Doküman Kodu	BİDB-BGYS-02
	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- 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 ilişkisi kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

3.7.1. 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 ilişkisi 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 boşa kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmelidir.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

3.7.2. Acil Erişim Yetkilendirme Yönetimi

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

3.8. Kablosuz İletişim Politikası

- Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınmalıdır.
- Bütün kablosuz erişim cihazları BİDB tarafından onaylanmış olmalı ve BİDB'nin belirlediği güvenlik ayarlarını kullanmalıdır.
- 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.
- Erişim cihazlarındaki firmwareler düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlamaktadır.
- Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.

	NUH NACİ YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- f) Varsayılan SSID isimleri kullanılmamalıdır. SSID ayarı bilgisi içerisinde kurumla ilgili bilgi olmamalıdır, mesela kurum ismi, ilgili bölüm, çalışanın ismi vb.
- g) Radyo dalgalarının binanın dışına taşmamasına özen gösterilmelidir. Bunun için çift yönlü antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanmalıdır.
- h) 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.
- i) Erişim cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dâhil olmalıdırlar.
- j) Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından Kurum'un tüm internet bant genişliğinin tüketilmesi engellenmelidir.
- k) Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlı olmalıdır.
- l) Kullanıcı bilgisayarlarında kişisel antivirüs ve güvenlik duvarı yazılımları yüklü olmalıdır.
- m) Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

3.9. Yazılım Güvenliği Politikası

- 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 bulunduğu mesai saatleri dışında bir zaman diliminde devreye alınmalıdır.
- k) Kurum için geliştirilen uygulamalar, uluslararası kabul görmüş standartlara bağlı dokümanite edilmelidir. Uygulama için yazılmış olan dokümanlar uygulama ile beraber kuruma teslim edilmelidir.

	NUH NACİ YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

3.10. Yazılım Geliştirme Politikası

- Sistem yazılımında mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.
- Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.
- İhtiyaçlar, uygun bir şekilde tanımlanmalıdır.
- Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.
- Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.
- Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.
- 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.
- Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.
- Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.
- Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.
- Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.
- Yazılımlar sınıflandırılmalı / etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

3.11. Veritabanı Güvenlik Politikası

- Veritabanı sistemleri envanteri dokümante edilmeli ve bu envanterden sorumlu personel tanımlanmalıdır.
- Veritabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.
- Veritabanı sistem kayıtları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.
- Veritabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir.
- Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.
- Yedekleme planları dokümante edilmelidir.
- Manyetik kartuş, DVD veya CD ortamlarında tutulan log kayıtları en az 2 (iki) yıl süre ile güvenli ortamlarda saklanmalıdır.
- Veritabanı erişim politikaları “Kimlik Doğrulama ve Yetkilendirme” politikaları çerçevesinde oluşturulmalıdır.
- Hatadan arındırma, bilgileri yedekten dönme kuralları “Acil Durum Yönetimi” politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- 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 erişmemelidir.
- 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 kullanıcılar bağlanıp sorgu yapmamalıdır.
- bb) Veritabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir. (Ağ trafiğini dinleyen casus yazılımların verilere ulaşmaması 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.

	NUH NACİ YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

3.12. Donanım Güvenliği Politikası

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

3.13. Erişim Yönetimi ve Erişim Kayıtlarının Tutulması Politikası

Erişim yapan kullanıcıların yapmış oldukları işlemler loglanmalı, gerektiğinde erişim yetkilisinin kayıt silme logları da listelenebilir olmalıdır.

3.13.1. Erişim Yönetimi

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

- Sunuculara erişim için IP/SEC ya da SSL VPN kullanılmalıdır. Mümkünse kullanıcıların erişimi için SSL ve VPN tercih edilmelidir. Güvenlik Birimi tarafından sağlanmalıdır.
- Sunuculara kullanıcı erişimi için SSH, RDP gibi protokollerle sunucu yönetimi için belirli portlar erişim verilmelidir.
- Sunucuların kendi aralarında servis ve yönetimleri için belirli portlarla erişim sağlanması gerekmektedir.
- Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir. Parola yönetimi bilgi güvenliği politikası parola yönetim politikaları ile yürütülmelidir.
- Kullanıcıların sunucu yönetim için sağlanan erişimde merkezi kullanıcı yönetimi (MS AD, LDAP, ssh-key) ile yapılmalıdır.

	NUH NACİ YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- 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.

3.13.2. Kayıt Tutulması (Log tutulması)

- a) Kurumun güvenlik cihazlarına ait loglar güvenlik birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle iş birliği içinde raporlar paylaşılmalıdır.
- b) Kurumun veri tabanlarına ait loglar veri tabanları birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle iş birliği içinde raporlar paylaşılmalıdır.
- c) Kurumun network cihazlarına ait loglar network birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle iş birliği 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 istatistiksel 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.

3.14. 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.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- 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, dokümanite 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.

3.15. 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 evrak kırma 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 gerçekleştirilmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.
- d) İmha işlemi gerçekleştirilecek 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 gerçekleştirilen 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.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- 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 gerekmektedir.

3.16. Veri Yedekleme ve İş Sürekliliği Politikası

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.

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

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

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

3.17. Son Kullanıcı Güvenliği Politikası

- a) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.
- b) Kullanıcılara erişim haklarını açıklayan yazılı bildirimler 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 planlamaları 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 paylaşılması 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.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

3.18. Kişisel Verilerin Korunması ve İşlenmesi Politikası

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

3.18.1. Kişisel Verilerin Güvenliğinin Sağlanması

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

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- Kişisel verilerin muhafazasını sağlamak, için gerekli her türlü teknik ve idari tedbirleri alır.

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

3.18.2. Teknik Tedbirler

- BİDB, kurulan sistemler için gerekli iç kontrolleri yapar.
- Kurulan sistemler kapsamında risk analizi, veri sınıflandırması, bilgi güvenliği risk değerlendirmesi ve iş etki analizinin gerçekleştirilmesi süreçlerini işletir.
- Bu süreçler doğrultusunda teknolojiye gelişmelere uygun teknik önlemleri alır.
- 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.
 - Kamera kayıtlarına erişimde kullanıcı yetkilendirilmesi yapılır ve veriler güvenli ortamda saklanır.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

3.19. Bakım Politikası

- Kurum sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için gerekli anlaşmalar için yıllık bütçe ayrılmalıdır.
- Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.
- Sistem üzerinde yapılacak değişiklikler ile ilgili olarak “Değişim Yönetimi Politikası” ve ilişkili standartlar uygulanmalıdır.
- Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenmelidir.
- 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.
- Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda “Nuh Naci Yazgan Üniversitesi Bilgi Güvenlik Politikaları” uyarınca hareket edilmelidir.

3.20. Bilgi Güvenliği Teknik ve Farkındalık Eğitim Politikası

- Kurum içerisinde bilgi güvenliği teknik ve farkındalık eğitimleri için yıllık bir plan yapılmalıdır.
- Yıllık planlar çerçevesinde bilgi güvenliği teknik ve farkındalık eğitimleri gerçekleştirilmelidir.
- 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.

3.21. Basılı Çıktı ve Dağıtım Politikası

- Tüm kritik bilgisayar raporlarının; bilginin hassasiyet seviyesine göre bir güvenlik sınıflandırma değeri olacaktır. Sınıflandırmayı bilgi sahibi kendisi yapacaktır.
- Kâğıt ortamında basılı “Gizli” tanımlı raporların sadece hitap edilen kullanıcıya ulaştırılmasını güvence altına alacak metotlar belirlenecektir.
- Kritik raporların dökümünü alan kullanıcı, rapor içeriğindeki bilginin uygun bir şekilde korunmasından sorumludur.
- Herhangi bir kişi kendine ait olmayan kritik bir doküman bulur ise olay bildiriminde bulunur ve doküman ilgisine iletir.
- “Gizli Sınıflandırmasına tabi” kâğıt belgeleri kilitli dolap ve kasalarda muhafaza edilecektir.
- “Gizli Sınıflandırmasına tabi” kâğıt bilgileri faks ile ileilmeyecektir.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- g) “Gizli Sınıflandırmasına tabi” bilgi içeren çıktılar ağ ortamında paylaşılmış yazıcılardan yazdırılıyorsa yazdırma işini başlatan kullanıcı beklemeden yazdırılan belgenin bulunduğu alana gidecek ve çıktının başkaları tarafından görülmesine imkân vermeyecektir.

3.22. Bilgi Sınıflandırma Politikası

- 3.Taraf veya kuruluşun personeline yönelik tehlike arz eden herhangi bir ürün veya hizmet, bu tehlikenin doğasını açıklayacak biçimde tanımlanmalıdır.
- Tüm bilgiler, aksi onaylanmadığı sürece gizli bilgi olarak nitelendirilmelidir.
- Bir depolama ortamının çeşitli seviyelerde gizlilik içermesi durumunda, en yüksek gizlilik seviyesi içeren bilgiler öncelikli olarak kabul edilir.
- Kullanıcılar, BİDB'nin sağlamış olduğu olanaklar dahilinde kendi bilgisayarlarının yedeklerini almaktan veya aldirmaktan sorumludur.
- Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
- Sistemlere login olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir. Kullanıcı haklarını izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.
- Fotokopi cihazlarını kullanan Nuh Naci Yazgan Üniversitesi çalışanları cihazlar üzerinde bırakmış olduğu dokümanlardan sorumludur.
- Kişiler tarafından yazılmış herhangi bir resmi dokümanın silinmez mürekkeple yazılması ve uygun şekilde işaretlenmesi gerekir. Yapılacak herhangi bir değişikliğin altı çizilmeli, tarihlenmeli ve yeniden onaylanmalıdır.
- Gizli dokümanların tüm sayfaları numaralandırılmalıdır.

3.23. Bilgi ve Yazılım Alışverişi Politikası

- Organizasyon, elektronik transferlere yönelik log kayıtları tutulmakta olduğundan emin olmalıdır.
- Organizasyonun yazılımlarını veya verilerini kullanmakta olan üçüncü taraflar, gerekli koruma ölçütlerini içeren bir yazılı sözleşme imzalamalıdır. Böylece üçüncü tarafların söz konusu bilgiyi izinsiz kullanması, değiştirmesi veya çoğaltması engellenmiş olacaktır.
- Elektronik ortamda sözleşmenin yapıldığı üçüncü taraflarla, kâğıt üzerinde de anlaşma yapılmalıdır.
- Bilgi ve veri alışverişinden önce dış tarafların kimliklerinin tespit edilmesi gerekir.
- Üçüncü taraflara yollanan bilgisayar ortamı yeni olmalı veya herhangi bir bilgi içermemelidir.
- Yetkisi olmayan çalışanlar tarafından gönderilen e-postalar, organizasyonu bağlamaz.
- İş iletişiminin sağlanması için sadece organizasyon tarafından yetkilendirilen çalışanların e-posta adresleri kullanılmalıdır.
- Organizasyon web sitesinin korunması sağlanmalıdır.
- Gizli bilgiler sadece uygun veri sunucularında kayıt altına alınmalıdır.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- j) Yazılım yükleme veya yazılım güncellemelerini yapma ve sistem bakımını gerçekleştirme yetkisi sadece bilgi işlemdedir.
- k) Kritik bir dosyada çeşitli değişikliklerin yapılması durumunda, dosyanın yedeği alınmalıdır.
- l) Organizasyonda bilgi sistemleri aracılığı ile gönderilen mesajlar, saldırgan veya ayrımcılık içeren bildirimler içermemelidir. Organizasyonun bilgi sistemi sadece iş gereklilikleri için kullanılmalıdır.
- m) Bir e – posta gizlilik içermekte olduğuna dair bir not eklendiğinde, bu mesajı sadece e – postanın gönderildiği kişinin maili aldığından emin olunmalıdır.
- n) E – postalarda taranmış imzalar bulunmamalıdır.
- o) Organizasyonun çalışanları çeşitli tartışma gruplarına katılmamalıdır.
- p) E – posta yoluyla gönderilen bilgiler, bu bilginin kimden gelmekte olduğunu içermelidir.
- q) E – posta yoluyla gönderilen bilgiler, spesifik bir geri dönüş adresi içermelidir.
- r) Silinebilir ortamlara kaydedilmiş olan gizli bilgilerin kullanımdan sonra silinmesi gerekir.
- s) Gizlilik içeren bilgiler telefon aracılığı ile paylaşılmamalıdır.
- t) Çalışanlar gizlilik içeren bilgileri telesekreterlere veya sesli mesajlaşma sistemlerine kaydetmemelidir.
- u) Toplantılarda yapılan video konferanslar, yönetim veya katılımcılar tarafından izin verilmedikçe kaydedilmemelidir.
- v) İşle ilgili tüm aramalar kuruluş telefonları kullanımı ile yapılmalıdır.
- w) Gizlilik içeren bilgilerin umumi yerlerde konuşulmaması gerekir.
- x) Bilgi sistemleri sadece iş için kullanılmalıdır.

3.24. Değişim Yönetimi Politikası

- a) Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümanite edilmelidir.
- b) Yazılım ve donanım envanteri oluşturularak güncel tutulmalıdır.
- c) Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmelidir.
- d) Değişiklikler gerçekleştirilmeden önce BİDB en üst yöneticisinden onay alınmalıdır.
- e) Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.
- f) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.
- g) Teknoloji değişikliklerinin kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmelidir.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- h) Değişiklik yönetimini işletmek için bir talep yönetim sistemi kurmak ve işletmek önemlidir. Talebin nasıl alınacağı ve değerlendirileceği gibi esaslar tanımlanmalıdır.
- i) Değişiklik onayının, “hangi kontroller ne şekilde yapıldıktan sonra verileceği” tanımlanmalıdır.
- j) Değişiklik öncesi test süreci tanımlanmalıdır.
- k) Değişikliğin varlık kritikliğine göre yapılacağı zaman ve yöntemler tanımlanmalıdır.

3.25. Fiziksel Güvenlik Politikası

- a) Kurumsal bilgi varlıklarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilmelidir.
- b) Kurumsal bilgi varlıklarının dağılımı ve bulundurulmuş bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.
- c) Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlarına girişi yetkili görevliler gözetiminde gerçekleştirilmelidir.
- d) Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.
- e) Kritik sistemler erişim yetkisi ile belirlenmiş alanlarda bulundurulmalıdır.
- f) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalıdır.
- g) Kuruma giriş yapacak ziyaretçi veya kurye teslimatları yetkili görevliler gözetiminde gerçekleştirilmelidir.
- h) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.
- i) Fotoğraf, video, ses vb. kayıt cihazlarının yetki verilmeyen kişiler tarafından güvenli alanlara sokulması yasaklanmalıdır.

3.26. Kabul Edilebilir Kullanım Politikası

- a) Güvenlikten, Nuh Naci Yazgan Üniversitesi personeli, iş yapan yüklenici kurumlar ve ilgili tüm personel, kendi alanlarına ait güvenlik politikalarına uymak zorundadır.
- b) Güvenlik politika ve ekleri BİDB tarafından Nuh Naci Yazgan Üniversitesi çalışanlarına, yeni işe başlayanlara ve yüklenici kurumlara duyurulacaktır.
- c) Nuh Naci Yazgan Üniversitesi ortamında tutulan ve iletilen tüm bilgiler; kurumun malıdır ve bu bilgileri izleme ve denetleme hakkına sahiptir.
- d) Nuh Naci Yazgan Üniversitesinin gizli olarak belirlediği tüm bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. Kurumun iş gereksinimi dışında bu bilgilerin kopya edilmesi ve iletilmesi yasaktır.
- e) Nuh Naci Yazgan Üniversitesi personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş güvenlik cihazlarını korumaktan

	NUH NACİ YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

sorumludur. Erişim bilgileri herhangi birine söylenemez ve bu bilgiler başkaları ile paylaşamaz.

- f) Hiçbir personel, bilgisayarlarından anti virüs koruma yazılımını devre dışı bırakamaz.
- g) Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.
- h) Hiçbir personel izin almadan kendi PC' sinden veya başka bir kaynak kullanarak, Nuh Naci Yazgan Üniversitesinin Bilişim Ağını tarayamaz, izleyemez veya dinleyemez.
- i) Nuh Naci Yazgan Üniversitesi onaylı resmi penetrasyon testleri haricinde, bilgisayar sunucuları için içeriden veya dışarıdan port taraması yapılması yasaktır.
- j) Hiçbir personel, kurum içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.

3.27. Kriptografik Kontroller Politikası

- a) **Gizlilik:** Saklanan veya iletilen hassas veya kritik bilgiyi korumak için şifrelemenin kullanılması,
- b) **Bütünlük/Güvenilirlik:** Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için sayısal imzaların veya mesaj doğrulama kodlarının kullanılması,
- c) **İnkar edilemezlik:** Bir olay veya faaliyetin oluşumu veya oluşmadığının kanıtını elde etmek için kriptografik tekniklerin kullanılması.
- d) Personelin gönderdiği maillerde, hiçbir şekilde yönetici, kullanıcı gibi hesap şifreleri bulundurulmamalıdır.
- e) İnternete açık kritik veri içeren uygulamalara kriptolu (şifreli) bağlantı ile bağlanılmalı, kriptolu (şifreli) kullanmayan yöntemler tercih edilmemelidir. Düz metin kullanarak veri alışverişi yapan yöntemlerin kullandığı portlar gerekirse kapatılmalıdır.
- f) Kriptolu kullanımı ile hangi iş bilgisinin korunacağı ile ilgili genel prensipler belirlenmelidir.
- g) Taşınabilir ortam, cihaz ve iletişim hatlarında iletilen hassas bilginin korunması için şifreleme mekanizmalarının kullanımı belirlenmelidir.
- h) Organizasyon çapında etkin bir uygulama için uyarlanması gereken standartlar ortaya konulmalıdır.
- i) Kriptografik anahtarların korunması, şifrelenmiş bilginin kaybolması, tehlikeye düşmesi veya hasar görmesi durumunda tekrar geri alınması ile ilgili metotları içeren anahtar yönetimi uygulanmalıdır.
- j) Politikanın uygulanması, anahtar üretimini de içeren anahtar yönetimi ile ilgili görevler ve sorumluluklar belirlenmelidir.

	NUH NACI YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

3.28. Temiz Masa Temiz Ekran Politikası

- Çalışma sonunda kâğıt ortamında ya da elektronik cihazlar üzerinde tutulan “gizli ya da çok gizli” bilgiler güvenli ortamlarda (çelik kasa, kilitli güvenli ortamlar vb.) saklanmalıdır.
- Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler belirlenmiş yöntemlerle imha edilmelidir.
- Her türlü haberleşmede kullanılan cihazlar (telefon, faks, fotokopi makineleri) yetkisiz erişimlere bırakılmamalıdır. Cihazlar üzerinde belge, doküman bırakılmamalıdır.
- Her türlü ekrandan ulaşılabilen bilgiler, şifreler, anahtarlar ve kodlar, bilginin sunulduğu sistemler, ana makineler (sunucu), PC’ler vb. cihazlar şifresiz kullanılmamalıdır
- Ekranlarda çalışılmaması durumunda devreye girecek ekran koruması (parola) tüm PC’lerde, notebooklar da etkinleştirilmelidir.
- Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terk edilecekse ekran kilitlenmelidir. Bu işlem Windows + L tuşuna basılarak yapılabilir.
- Hassas bilgiler içeren evraklar, bilgi ve belgelerin masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulunmaması gereklidir.

3.29. Varlıklara Yönelik Sorumluluk Politikası

- Her sene bir bilgi sistemleri envanteri yapılmalı ve bu konuda görevlendirilmiş kişiye bu liste verilmelidir. Bu çalışmanın amacı kuruluşun varlıklarını tespit etmek ve bu varlıkların kaybedilmesinin engellenmesini sağlamaktır.
- Yeni üretilen bilginin bir sahibinin belirlenmesi ve bu bilginin uygun biçimde sınıflandırılması gerekir.
- Satın alınacak herhangi bir yazılım veya donanım BİDB ile satın alınması ve bilgi güvenliği standartları ile uyumlu olması gerekir.
- Organizasyonun sahip olduğu tüm sistemlerin yönetimi, kullanıcı ayrıcalıklarının takibi ve erişim kontrol loglarının izlenmesi BİDB tarafından yapılmalıdır.

3.30. Ziyaretçi Kabul Politikası

- Dışarıdan ziyaret amaçlı gelen kişiler kuruluş girişinde güvenlik tarafından karşılanır ve ziyaret edeceği idarecinin onayı ile kuruluşa kabulü yapılır.
- Gelen ziyaretçi Başkan Seviyesinde ziyaret gerçekleştiriyorsa Güvenlik tarafından ziyarete geldiği kişiye kadar getirilir.
- Ziyaretçiler sadece toplantı odalarında ve personel odalarında ağırlanır.
- Dışarıdan ziyaret amaçlı gelen kişiler yönetim ofisleri, arşiv odası ve sistem odası gibi yerlere alınmamalıdır.
- Kargo elemanları teslimatlarını güvenliğe teslim etmelidirler. Bunun dışında kuruluşa girişleri yasaktır.

	NUH NACİ YAZGAN ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ POLİTİKASI	Doküman Kodu	BİDB-BGYS-02
		Yürürlük Tarihi	21/11/2019
		Revizyon Tarihi/No.	01/12/2021/01

- f) Ziyarete gelen kişiler ile ilgili bilgiler Güvenlik tarafından ziyaretçi takip sistemi ile kaydedilir.

3.31. Taşınabilir Cihaz Politikası

- Her çalışan kendisine zimmetlenen taşınabilir cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.
- Kuruluşa bilgisayar, taşınabilir bellek ve taşınabilir cihazlara dışarıdan herhangi bir yazılım, siyasi propaganda, ırkçılık, şiddet, pornografî veya erotizm içeren resim, film veya müzik kopyalanamaz ve cihaz içerisinde bulundurulamaz.
- Kuruluş telefon hatları ve bilgisayarlar üzerinden üçüncü taraf kişilerle borç alacak ilişkisi, tehdit, küfür, kuruluş itibarını zedeleyecek şeyler ve yasa dışı olan iletişim kurulamaz.
- Taşınabilir cihazlar üzerindeki anti virüs programları hiçbir nedenle devre dışı bırakılmaz.
- Taşınabilir cihazlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar olanaklar dahilinde ağ üzerinde ilgili adrese kaydedilmelidir.
- Kaybolması ve çalınması kolay olduğundan taşınabilir cihazlar başıboş bırakılmamalıdır.

4. Diğer Hükümler

4.1. Uygulama ve Yaptırım

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.