Ege Üniversitesi Alan Adı ve Barındırma Hizmetleri Politikası

Politika Numarası: BT-POL-001
Yürürlük Tarihi:
Revizyon Numarası: 1.0
Sorumlu Birim: Bilgi İşlem Daire Başkanlığı (BİDB)

Giriş: Politikanın Amacı, Dayanağı ve Kapsamı

Amaç

Bu politikanın temel amacı, Ege Üniversitesi'nin sahip olduğu ege.edu.tr internet alan adı ve buna bağlı alt alan adlarının tahsisi ile Bilgi İşlem Daire Başkanlığı (BİDB) tarafından sunulan web ve sunucu barındırma hizmetlerinin kullanımına ilişkin ilke, kural ve sorumlulukları belirlemektir. Politika, üniversitenin dijital varlıklarının kurumsal kimlikle uyumlu, güvenli, erişilebilir ve sürdürülebilir bir yapıda yönetilmesini sağlamayı hedefler. Bu standartlaşma hem hizmet taleplerinde verimliliği artıracak hem de üniversite kaynaklarının adil ve planlı bir şekilde dağıtılmasını temin edecektir. Tutarlı ve yapılandırılmış bir yaklaşım, web sitelerinin üniversitenin güvenlik, erişilebilirlik ve içerik standartlarına uygunluğunu sağlamak için kritik öneme sahiptir.

Dayanak

Bu politika, 2547 sayılı Yükseköğretim Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yayımlanan İnternet Alan Adları Yönetmeliği ve .tr Ağ Bilgi Sistemi (TRABİS) kurallarının ilgili kararlarına dayanılarak hazırlanmıştır. ege.edu.tr uzantılı alan adlarının tahsisi, Yükseköğretim Kurulu (YÖK) tarafından tanınan yükseköğretim kurumlarına özel olup, başvuru süreçleri TRABİS tarafından belirlenen belgelendirme usullerine tabidir.

Kapsam

Bu politika, Ege Üniversitesi bünyesindeki tüm akademik ve idari birimleri, araştırma merkezlerini, laboratuvarları, üniversite tarafından tanınan öğrenci kulüplerini, akademik/idari projeleri, bilimsel etkinlikleri (konferans, sempozyum vb.) ve bu birimlere hizmet veren tüm personeli kapsar. Politika, ege.edu.tr altındaki tüm alan adı tahsislerini ve BİDB Veri Merkezi'nde sunulan tüm web/sunucu barındırma hizmetlerini (paylaşımlı barındırma, sanal sunucu vb.) düzenler.

Bölüm 1: Tanımlar ve Terminoloji

Bu politika metninde tutarlılığı sağlamak ve yanlış anlaşılmaları önlemek amacıyla kritik terimler aşağıda tanımlanmıştır:

- **BİDB (Bilgi İşlem Daire Başkanlığı):** Üniversitenin merkezi BT altyapısını yöneten ve bu politika kapsamındaki hizmetleri sunan, denetleyen ve koordine eden birimdir. [9]
- **Alan Adı (Domain Name):** Bir internet kaynağını (örneğin bir web sitesi) tanımlayan, ege.edu.tr gibi benzersiz, alfanümerik bir isimdir. Alan adları, noktalarla ayrılmış ve sağdan sola doğru hiyerarşik olarak inen seviyelerden oluşur. [1]
- **Üçüncü Seviye Alan Adı (Third-level Domain):** ege.edu.tr alan adının hemen solunda yer alan ve genellikle fakülte, enstitü, daire başkanlığı gibi ana kurumsal birimleri tanımlayan isimdir. Örnek: bidb.ege.edu.tr.
- **Barındırma (Hosting):** Web sitelerinin, uygulamaların veya diğer dijital servislerin internet üzerinden 7/24 erişilebilir olmasını sağlayan sunucu altyapısı ve ilgili teknik hizmetlerin bütünüdür.
- **Hizmet Sahibi (Service/Site Owner):** Alan adı ve/veya barındırma hizmetini talep eden birimin idari amiridir (Dekan, Enstitü Müdürü, Daire Başkanı vb.). Hizmetin kurumsal hedeflere uygunluğundan, içeriğinden ve bu politikaya uyumundan nihai olarak sorumludur. Bu kişinin tam zamanlı bir üniversite personeli olması zorunludur.
- **Teknik Sorumlu (Webmaster/Custodian):** Hizmet Sahibi tarafından atanan ve web sitesinin/uygulamanın günlük teknik yönetiminden, içerik güncellemelerinden, kullanıcı yönetiminden ve operasyonel güvenliğinden sorumlu olan personel veya öğrenci çalışandır.
- **Kabul Edilebilir Kullanım Politikası (AUP):** Üniversitenin bilgi teknolojileri kaynaklarının hangi amaçlarla, ne şekilde ve kimler tarafından kullanılabileceğini tanımlayan, yasa dışı, etik dışı ve kurumsal misyona aykırı faaliyetleri yasaklayan kurallar bütünüdür.
- **Hizmet Seviyesi Anlaşması (SLA):** BİDB ile Hizmet Sahibi arasında, sunulan hizmetin kalitesi, erişilebilirliği (uptime), destek süreleri ve tarafların karşılıklı sorumluluklarını şeffaf ve ölçülebilir bir şekilde tanımlayan resmi anlaşmadır.

- **TRABİS (.tr Ağ Bilgi Sistemi):** Türkiye'nin .tr uzantılı internet alan adlarının yönetimini, tahsisini ve kayıt işlemlerini merkezi olarak yürüten, BTK tarafından kurulan sistemdir.

Bölüm 2: Alan Adı Tahsis Kuralları ve Prosedürleri

Bu bölüm, üniversitenin en değerli dijital varlıklarından olan alan adlarının adil, tutarlı ve stratejik bir şekilde yönetilmesini sağlamayı amaçlar. Alan adı tahsis süreci, üniversitenin kurumsal kimliğini ve dijital itibarını koruyacak şekilde yapılandırılmıştır.

2.1 Alan Adı Başvurusu İçin Uygunluk Kriterleri

Alan adı talepleri yalnızca aşağıda listelenen kurumsal yapılar için kabul edilir. Bireysel veya kişisel web sayfaları için özel alan adı tahsis edilmez. Bu kural, kişisel web sayfalarının kurumsal birimlerle karıştırılmasını önlemeyi amaçlar. Ayrıca, kişilerin bireysel projelerine ait web sayfası talepleri de ulusal ve uluslararası hibeler kapsamında gerçekleştirilen yaygınlaştırma faaliyetleri adı altında proje web sayfası açılması ve yönetilmesi hizmeti kurumsal yapı dışında değerlendirildiğinden alan adı tahsisi kapsamında **kabul görmeyecektir**.

- **Akademik Birimler:** Fakülteler, enstitüler, yüksekokullar, bölümler, anabilim dalları.
- **İdari Birimler:** Daire başkanlıkları, müdürlükler, rektörlüğe bağlı birimler.
- **Araştırma ve Uygulama Merkezleri/Laboratuvarları:** Üniversite Senatosu tarafından resmi olarak tanınmış ve faaliyetleri devam eden merkezler ve laboratuvarlar.
- **Bilimsel Etkinlikler:** Üniversite tarafından düzenlenen veya ev sahipliği yapılan konferans, sempozyum, çalıştay gibi süreli etkinlikler.
- **Öğrenci Kulüpleri:** Üniversite Sağlık, Kültür ve Spor Daire Başkanlığı tarafından resmi olarak tanınan ve aktif statüde olan öğrenci kulüpleri.

2.2 Başvuru ve Onay Süreci

Tüm alan adı ve barındırma talepleri, şeffaf ve izlenebilir bir süreçle yönetilir. Süreç, talebin kurumsal uygunluğunu ve teknik gereksinimlerini doğrulamayı hedefler.

1. **Resmi Başvuru:** Tüm talepler, ilgili birimin en üst amiri (Hizmet Sahibi) tarafından onaylanmış resmi bir yazı ile Elektronik Belge Yönetim Sistemi (EBYS) üzerinden BİDB'ye iletilir.
2. **Talep Formu:** Başvuru yazısının ekinde, "Alan Adı ve Barındırma Talep Formu" eksiksiz olarak doldurulmuş halde bulunmalıdır. Formda aşağıdaki bilgiler yer almalıdır:
    - Talep edilen alan adı ve en az iki alternatif.
    - Alan adının kullanım amacı, hedef kitlesi ve faaliyetin süresi.

- Hizmet Sahibi ve Teknik Sorumlu'nun güncel iletişim bilgileri.
- Talep edilen hizmetin türü (sadece alan adı yönlendirme, web barındırma, sanal sunucu vb.).
- Barındırma hizmeti talep ediliyorsa, ihtiyaç duyulan teknik özellikler (işletim sistemi, depolama alanı, veri tabanı türü vb.).

3. **Değerlendirme:** BİDB, talebi bu politikada belirtilen isimlendirme ve uygunluk kriterlerine göre inceler. Gerekli durumlarda başvuru sahibiyle iletişime geçerek revizyon veya ek bilgi talep edebilir.

2.3 Alan Adı Hiyerarşisi ve İsimlendirme Standartları

Alan adı hiyerarşisi, sadece teknik bir düzenleme değil, aynı zamanda üniversitenin kurumsal yapısının dijital bir yansımasıdır. Üçüncü seviye alan adları, üniversitenin ana "vitrinlerini" oluşturur ve bu nedenle sıkı bir şekilde kontrol edilmelidir. Dördüncü seviye alan adları ise bu ana birimlerin altındaki faaliyetler için esneklik sağlar. Bu yapı hem marka bütünlüğünü korur hem de dijital karmaşayı (domain sprawl) önler. [isim].ege.edu.tr şeklindeki bir alan adı, kullanıcı nezdinde kurumsal ve resmi bir algı yaratır. Kısa ömürlü bir proje veya küçük bir laboratuvar için bu seviyede bir alan adı tahsisi, bu algıyı zayıflatır ve kafa karışıklığına yol açar. Bu durum, kurumsal kimliğin ve dijital marka değerinin korunması için hiyerarşik bir isimlendirme politikasını zorunlu kılar.

- **Üçüncü Seviye Alan Adları ([isim].ege.edu.tr):** Bu seviye, yalnızca Fakülte, Enstitü, Yüksekokul, Daire Başkanlığı gibi kalıcı ve ana akademik/idari birimlere tahsis edilir. İsim, birimin resmi adını açıkça yansıtmalı ve genel kamuoyu tarafından anlaşılmayan kısaltmalardan kaçınılmalıdır (örn: muhendislik.ege.edu.tr, personel.ege.edu.tr). Çok genel ("generic") isimler (örn: arastirma.ege.edu.tr, egitim.ege.edu.tr) BİDB ve Kurumsal İletişim Koordinörlüğü'nün ortak kararı olmadan tahsis edilemez, çünkü bu tür isimler tüm üniversiteyi kapsayan bir faaliyeti ima eder.
- **Dördüncü Seviye Alan Adları ([isim]-[birim].ege.edu.tr):** Bölümler, laboratuvarlar, projeler, etkinlikler ve öğrenci kulüpleri gibi alt birimler için standarttır. Bu yapı, aidiyeti net bir şekilde belirtir ve kurumsal hiyerarşiyi yansıtır (örn: bilgisayar-muhendislik.ege.edu.tr, robotik-makine.ege.edu.tr, icra2025.ege.edu.tr).
- **Genel İsimlendirme İlkeleri:**
  - Alan adları, temsil ettiği birimi veya faaliyeti açık, net ve yanıltıcı olmayacak şekilde tanımlamalıdır.
  - Mümkün olduğunca kısaltmalardan kaçınılmalıdır. Kamuoyunca bilinmeyen kısaltmalar kullanılmamalıdır.
  - Alan adları sadece küçük harf (a-z), rakam (0-9) ve tire (-) içerebilir. Tire ile başlayamaz veya bitemez. Boşluk ve diğer özel karakterler kullanılamaz.
  - Saldırgan, aşağılayıcı, yasa dışı veya üniversitenin itibarına zarar verecek ifadeler içeren alan adları kesinlikle kabul edilemez.

- Kişi adları, üçüncü seviye alan adı olarak tek başına kullanılamaz (örn: ahmet-yilmaz.ege.edu.tr yasaktır). Ancak bir program, merkez veya bina adı içinde geçebilir (örn: ahmet-yilmaz-burs-programi.ege.edu.tr).

Aşağıdaki tablo, doğru ve yanlış isimlendirme pratiklerini somutlaştırmak amacıyla hazırlanmıştır. Bu tablo, başvuru sahiplerinin daha ilk adımda doğru isimlendirme talebinde bulunmalarını teşvik ederek BİDB'ye gelen hatalı başvuru sayısını azaltmayı ve değerlendirme sürecini hızlandırmayı hedefler.

Birim/Faaliyet Türü	Kabul Edilebilir İsimlendirme (Doğru)	Kabul Edilemez İsimlendirme (Yanlış)	Gerekçe
Mühendislik Fakültesi	muhendislik.ege.edu.tr	mf.ege.edu.tr	Kısaltma kullanımı dış paydaşlar için kafa karıştırıcıdır.
Bilgisayar Müh. Bölümü	bilgisayar-muhendislik.ege.edu.tr	bilgisayar.ege.edu.tr	Aidiyet (Fakülte) belirtilmemiştir. 3. seviye alan adı ihlali.
Yapay Zeka Laboratuvarı	yapayzeka-bilgisayar-muhendislik.edu.tr	ai-lab.ege.edu.tr	Hiyerarşi yanlıştır ve kısaltma belirsizdir.
Uluslararası Robotik Konf.	robotik2025.ege.edu.tr	konferans.ege.edu.tr	İsim çok genel ve etkinliğe özgü değil.
Fotoğrafçılık Kulübü	Fotografcilik-kulup.ege.edu.tr	fotokulup.ege.edu.tr	Hiyerarşi yanlıştır ve "kulüp" aidiyeti belirsizdir.

2.4 Alan Adı Yenileme, Devir ve İptal Prosedürleri

- **Geçerlilik ve Yenileme:** Alan adları, tahsis edildikleri amaç için kullanıldıkları sürece geçerlidir. Proje veya etkinlik gibi süreli faaliyetler için tahsis edilen alan adları, faaliyet bitiminde BİDB tarafından geri alınır ve ilgili içerik yürütücü tarafından arşivlenir.
- **Kullanım Dışı Kalma:** Bir alan adının veya barındırma hizmetinin en az bir (1) yıl boyunca aktif olarak kullanılmaması (web sitesinin güncellenmemesi, erişilemez olması) durumunda, BİDB Hizmet Sahibini uyarır. Otuz (30) gün içinde geçerli bir gerekçe sunulmazsa veya site aktif hale getirilmezse, BİDB hizmeti askıya alma veya sonlandırma hakkını saklı tutar.
- **Devir ve İptal:** Bir birimin adının değişmesi veya yeniden yapılanması durumunda, eski alan adı yeni alan adına belirli bir süre (genellikle 1 yıl) yönlendirilir ve ardından kullanımdan kaldırılır. BİDB, bu politikaya aykırı kullanım, güvenlik ihlali veya üniversitenin genel çıkarlarıyla çatışma durumunda, önceden bildirimde bulunarak bir alan adını veya

barındırma hizmetini geri alma veya iptal etme hakkın ı saklı tutar.

Bölüm 3: Web ve Sunucu Barındırma Hizmetleri

Bu bölüm, BİDB tarafından sunulan barındırma hizmetlerinin teknik çerçevesini, sınırlarını ve hizmet seviyesi taahhütlerini tanımlar.

3.1 Hizmet Modelleri

BİDB, üniversite birimlerinin farklı teknik ihtiyaçlarına göre çeşitlendirilmiş barındırma hizmet modelleri sunar. Tüm yeni web sitesi talepleri, BİDB tarafından yönetilen merkezi barındırma hizmetlerini kullanmak zorundadır. Harici barındırma hizmetlerini n kullanımı, yalnızca BİDB'nin sağlayamadığı özel bir teknik gereksinim olması durumunda ve BİDB'den alınacak yazılı istisnai izin ile mümkündür. Bu kural, üniversite verilerinin güvenliğini, bütünlüğünü ve merkezi yönetimini sağlamak için esastır.[11]

- **Katma n 1: Paylaşımlı Web Barındırma (Kurumsal Şablon):** Standart kurumsal web siteleri (fakülte, bölüm, idari birim vb.) için önerilen ve varsayılan hizmettir. BİDB tarafından yönetilen, güncellenen ve güvenliği sağlanan merkezi bir İçerik Yönetim Sistemi üzerinde çalışır. Kurumsal kimliğe uygun temalar, eklentiler ve temel güvenlik önlemleri BİDB tarafından sağlanır.
- **Katman 2: Gelişmiş Paylaşımlı Barındırma:** Özel PHP/MySQL veya.NET/MSSQL tabanlı uygulamalara ihtiyaç duyan birimler için sunulur. Sunucu altyapısı yönetimi BİDB'ye, işletim sistemi ve uygulama katmanının (kod, eklentiler vb.) yönetimi ile güvenliği ise hizmeti alan birime aittir.
- **Katman 3: Özel Sunucu:** Kök (root) veya yönetici erişimi gerektiren, özel yazılım ve yapılandırmalara ihtiyaç duyan karmaşık uygulamalar veya araştırma projeleri için talep eden birim tarafından temin edilen donanım kullanılır. Bu hizmet modelinde, sunucunun işletim sistemi dahil tüm yönetimi, güncellemeleri, yedeklemesi ve güvenliği tamamen hizmeti talep eden birimin sorumluluğundadır.

3.2 Teknik Altyapı ve Standartlar

- Sunulan hizmetlerin güncel teknik özellikleri (desteklenen PHP/MySQL sürümleri, depolama kotaları, CPU/RAM limitleri vb.) BİDB web sitesinde yayınlanır ve teknolojik gelişmelere paralel olarak periyodik olarak güncellenir.

- Tüm barındırma hizmetlerinde, BİDB tarafından sağlanan ve yönetilen SSL/TLS sertifikaları ile HTTPS üzerinden güvenli iletişim zorunludur. Bu, veri gizliliğini ve bütünlüğünü sağlamak için temel bir güvenlik standardıdır.
- Hizmetler, BİDB Veri Merkezi'nde, yedekli güç, iklimlendirme ve ağ altyapısına sahip sunucular üzerinde barındırılır, bu da hizmet sürekliliğini en üst düzeye çıkarmayı hedefler.

3.3 Yedekleme, Güvenlik ve Bakım Politikaları

- **Yedekleme:** BİDB, yönetimi altındaki sunucuların (Katman 1 ve 2) düzenli olarak (genellikle günlük ve haftalık) yedeklerini alır. Yedekler belirli bir süre saklanır (örn: günlükler 7 gün, haftalıklar 4 hafta). Birimin kendi hatasından kaynaklanan veri kayıplarında, yedekten geri dönüş işlemi BİDB'nin iş y oğunluğuna bağlı olarak yapılabilir. “Özel Barındırma” hizmetinde yedekleme sorumluluğu birime aittir.
- **Planlı Bakım:** BİDB, altyapıdaki güvenlik zafiyetlerini gidermek ve performansı artırmak için düzenli olarak planlı bakım çalışmaları yapar. Bu çalışmalar , hizmet kesintisine yol açacaksa, en az 72 saat öncesinden tüm hizmet sahiplerine e-posta ve/veya EBYS yoluyla duyurulur.
- **Acil Bakım:** Kritik güvenlik güncellemeleri (zero -day zafiyetleri vb.) söz konusu olduğunda, BİDB önceden haber verilmeksizin acil bakım ve yama uygulama hakkını saklı tutar.

3.4 Hizmet Seviyesi Taahhütleri (SLA)

Net bir Hizmet Seviyesi Anlaşması (SLA), sadece bir teknik metrik belgesi değil, aynı zamanda bir beklenti yönetimi aracıdır. Bu anlaşma, BİDB'nin hangi hizmetleri garanti ettiğini, hangi durumlarda "en iyi çaba" prensibiyle çalıştığını açıkça ortaya koyar . Bu şeffaflık, birimlerin BİDB'den gerçekçi beklentilere sahip olmasını sağlar ve BİDB üzerindeki operasyonel baskıyı azaltır. Ayrıca, BİDB'nin kaynaklarını (personel zamanı vb.) kritik ve acil görevlere önceliklendirmesi için resmi bir çerçeve sunar. BİD B tarafından sunulan hizmetlerin detaylı SLA'sı Ek B'de belirtilmiştir. Bu anlaşma asgari olarak şunları içerir:

- **Hizmet Erişilebilirliği (Uptime):** BİDB altyapısından kaynaklanan sorunlar için hedeflenen aylık erişilebilirlik oranı (örn: %99,5).
- **Destek Saat leri ve Yanıt Süreleri:** Destek taleplerinin alınabileceği saatler (mesai saatleri) ve talebin ciddiyetine göre ilk yanıt verme süreleri (örn: Kritik arıza- 1 saat, Normal talep- 8 iş saati).
- **Hariç Tutulan Durumlar:** Planlı bakımlar, hizmeti alan birimin kod/uygulama hataları, üçüncü parti hizmetlerdeki kesintiler ve mücbir sebepler SLA kapsamı dışındadır.

Bölüm 4: Roller, Sorumluluklar ve Mülkiyet

Bu bölüm, hizmetin yaşam döngüsü boyunca BİDB ve hizmeti alan birimlerin görev ve sorumluluklarını net bir şekilde ayırarak olası belirsizlikleri ortadan kaldırmayı hedefler.

4.1 Bilgi İşlem Daire Başkanlığı'nın (BİDB) Sorumlulukları

- Sunucu altyapısının fiziksel ve ağ güvenliğini sağlamak.
- Sunucuların kesintisiz güç kaynağı, iklimlendirme ve internet erişimin i temin etmek.
- İşletim sistemi ve BİDB tarafından kurulan temel yazılımların (web sunucusu, veritabanı vb.) yama ve güncellemelerini yapmak (Katman 1 ve 2 hizmetler için).
- Altyapıyı düzenli olarak yedeklemek ve felaket kurtarma planlarını güncel tutmak (Katman 1 ve 2).
- Hizmetlerle ilgili temel altyapı desteğini SLA'da belirtilen süreler içinde sağlamak.

4.2 Hizmet Sahibinin ve Teknik Sorumlunun Sorumlulukları

- Web sitesinde/uygulamada yayınlanan tüm içeriğin doğruluğundan, güncelliğinden ve yasalara (Telif Hakkı, KVKK vb.) uygunluğundan sorumludur.
- Web sitesinin/uygulamanın kendisi tarafından kurulan veya geliştirilen bileşenlerinin (CMS, eklentiler, temalar, özel kodlar) güvenliğini sağlamak ve güncellemelerini düzenli olarak yapmak.
- Kullanıcı hesaplarını ve yetkilerini yönetmek, zayıf parolalara izin vermemek ve kullanılmayan hesapları düzenli olarak temizlemek.
- BİDB tarafından bildirilen güvenlik zafiyetlerini veya politika ihlallerini belirtilen süre içinde gidermek.
- Web sitesinin üniversitenin Kurumsal Kimlik ve Marka Standartları ile Erişilebilirlik Politikası'na uygun olmasını sağlamak.
- Hizmet Sahibi ve Teknik Sorumlu bilgilerindeki değişiklikleri BİDB'ye derhal bildirmek.

4.3 Veri ve İçerik Mülkiyeti

- Barındırma h izmeti kapsamında sunucularda saklanan tüm veri ve içeriğin mülkiyeti, hizmeti talep eden birime aittir. Üniversite, bu içeriği yasal ve politikaya uygunluk

açısından denetleme hakkını saklı tutar ancak içeriğin sahibi değildir.

- Hizmetin sonlandırılması durumunda, birim kendi verilerini ve içeriğini yedekleyip almakla yükümlüdür. BİDB, hizmet sonlandıktan sonra 30 gün süreyle verileri saklar ve bu sürenin sonunda kalıcı olarak siler.

Aşağıdaki Rol ve Sorumluluk Matrisi (RACI Modeli), bir web sitesinin yaşam döngüsündeki temel görevlerde kimin hangi rolde olduğunu netleştirmek için tasarlanmıştır. Bu matris, "Bu kimin sorumluluğundaydı?" sorusundan kaynaklanan belirsizlikleri ortadan kaldırarak, görevlerin zamanında ve doğru kişi tarafından yapılmasını sağlar. Bu, özellikle bir güvenlik olayı veya kritik bir arıza anında hızlı ve koordineli hareket etmek için hayati bir araçtır.

Görev/Süreç	BİDB	Hizmet Sahibi	Teknik Sorumlu
Sunucu İşletim Sistemi Yamalama	Sorumlu (R)/Hesap Veren (A)	Bilgilendirilen (I)	Bilgilendirilen (I)
Web Sitesi İçeriğinin Güncellenmesi	Bilgilendirilen (I)	Hesap Veren (A)	Sorumlu (R)
CMS Çekirdek/Eklenti Güncellemesi	Danışılan (C)	Hesap Veren (A)	Sorumlu (R)
Kullanıcı Yetki Yönetimi	Bilgilendirilen (I)	Hesap Veren (A)	Sorumlu (R)
Veritabanı Yedeklemesi (Altyapı)	Sorumlu (R)/Hesap Veren (A)	Bilgilendirilen (I)	Bilgilendirilen (I)
Güvenlik İhlali Tespiti ve Raporlama	Sorumlu (R)	Hesap Veren (A)	Danışılan (C)/Bilgilendirilen (I)
KVKK Uyumunun Sağlanması	Danışılan (C)	Hesap Veren (A)	Sorumlu (R)
Alan Adı Yenileme Talebi	Bilgilendirilen (I)	Hesap Veren (A)	Sorumlu (R)

Not: R: Responsible (Sorumlu), A: Accountable (Hesap Veren), C: Consulted (Danışılan), I: Informed (Bilgilendirilen)

Bölüm 5: İçerik Standartları ve Kabul Edilebilir Kullanım Politikası (AUP)

Bu bölüm, üniversite ağında ve sunucularında barındırılan içeriğin uyması gereken standartları ve yasaklanan faaliyetleri tanımlar.

5.1 Kurumsal Kimlik ve Marka Standartlarına Uyum

- Tüm web siteleri, Üniversite Kurumsal İletişim Koordinatörlüğü tarafından belirlenen logo kullanımı, renk paleti, tipografi ve genel tasarım ilkelerine uymak zorundadır.

- Web sitelerinin altbilgi (footer) bölümünde üniversitenin resmi adı, sorumlu birimin adı, iletişim bilgileri ve "Tüm Hakları Saklıdır" ifadesi gibi standart kurumsal bilgilere yer verilmelidir.

5.2 Erişilebilirlik Standartları

- Tüm web siteleri, engelli kullanıcıların da içeriğe tam erişimini sağlamak amacıyla uluslararası kabul görmüş Web İçeriği Erişilebilirlik Yönergeleri'ne (WCAG) en az "AA" seviyesinde uymak zorundadır. Bu, resimler için alternatif metinler, videolar için altyazılar, klavye ile gezilebilir menüler ve yeterli renk kontrastı gibi unsurları içerir.

5.3 Yasaklanmış İçerik ve Faaliyetler

Kabul Edilebilir Kullanım Politikası (AUP), sadece yasa dışı faaliyetleri engellemekle kalmaz, aynı zamanda üniversitenin temel misyonunu ve kâr amacı gütmeyen statüsünü korumayı hedefler. Ticari faaliyetlerin ve siyasi propagandanın yasaklanması, üniversite kaynaklarının eğitim ve araştırma dışı amaçlarla kullanılmasını önleyerek kurumu yasal ve finansal risklerden korur. Üniversiteye ait bir alan adı (ege.edu.tr) ve sunucu üzerinde kişisel bir e-ticaret sitesi işletmek veya bir siyasi parti için kampanya yürütmek, bu kaynakların misyon dışı kullanımına girer ve üniversitenin vergi muafiyeti statüsünü riske atabilir. Bu nedenle, AUP'nin bu tür faaliyetleri net ve kesin bir dille yasaklaması, sadece bir BT kuralı değil, aynı zamanda kurumsal bir risk yönetim stratejisidir.
Aşağıdaki içeriklerin ve faaliyetlerin üniversite sunucularında barındırılması veya üniversite alan adları üzerinden yayınlanması kesinlikle yasaktır:

- **Ticari Faaliyetler:** Kişisel veya üçüncü taraflar adına kâr amacı güden her türlü ürün veya hizmet satışı, reklam veya tanıtım. Üniversitenin resmi e-ticaret faaliyetleri bu kapsamın dışındadır ve Bölüm 6.3'teki özel kurallara tabidir.
- **Yasa Dışı Faaliyetler:** Yürürlükteki T.C. kanunlarına aykırı her türlü içerik (nefret söylemi, terör propagandası, yasa dışı madde kullanımı teşviki vb.).
- **Siyasi Propaganda:** Herhangi bir siyasi parti veya adayı destekleyen veya karşısında olan kampanya materyalleri.
- **Fikri Mülkiyet İhlalleri:** Telif hakkı, patent veya ticari marka hakları ihlal eden müzik, film, yazılım veya diğer materyallerin izinsiz paylaşımı.
- **Zararlı ve Rahatsız Edici İçerik:** Şiddet, pornografi, taciz, iftira veya özel hayatın

gizliliğini ihlal eden içerikler.

- **Ağ ve Sistem Bütünlüğünü Tehdit Eden Faaliyetler:** Kripto para madenciliği, botnet komuta-kontrol sunucuları, kimlik avı (phishing) siteleri veya zararlı yazılım dağıtımı.

5.4 Telif Hakları ve Fikri Mülkiyet

Web sitesinde kullanılan tüm metin, görsel, video ve diğer materyallerin telif haklarına uygun olması Hizmet Sahibinin sorumluluğundadır. Lisanssız veya izinsiz materyal kullanımından doğacak tüm yasal sorumluluk **Hizmet Sahibine** aittir.

Bölüm 6: Bilgi Güvenliği, Veri Koruma ve Uyumluluk

Bu bölüm, üniversitenin bilgi varlıklarını korumak, yasaluyumluluğu sağlamak ve siber tehditlere karşı dayanıklılığı artırmak için gereken güvenlik standartlarını belirler.

6.1 Veri Sınıflandırma ve İşleme Kuralları (KVKK Uyumu)

- Web sitelerinde işlenen ve saklanan tüm veriler, Üniversitenin Veri Sınıflandırma Politikası'na göre "Genel", "Hassas" veya "Gizli" olarak sınıflandırılmalıdır.
- 6698 sayılı KVKK kapsamında kişisel veri (öğrenci, personel veya üçüncü şahıslara ait kimlik, iletişim, sağlık bilgileri vb.) içeren web uygulamaları, BİDB'ye bildirilmek ve BİD B Güvenlik Birimi'nden onay almak zorundadır. Bu tür uygulamalar, yasal olarak zorunlu olan Aydınlatma Metni ve Açık Rıza mekanizmalarını içermelidir.
- Bilgi güvenliği politikamız gereği, sunucular üzerinde sıkıştırmış dosya formatları (.rar, .zip, .tar, vb .) ile yedek dosyaların bulundurulması güvenlik zafiyeti olarak değerlendirilmektedir. Bu dosya türlerinin tespiti halinde, BİDB tarafından ilgili dosyalar sistemden herhangi bir bildirim yapılmaksızın silinecektir.
- "Hassas" ve "Gizli" olarak sınıflandırılan verilerin, BİDB tarafından güvenliği onaylanmamış paylaşımlı barındırma ortamlarında saklanması yasaktır.

6.2 Güvenli Yazılım Geliştirme ve Yapılandırma Standartları

Güvenlik, sonradan eklenen bir katman değil, geliştirme sürecinin ayrılmaz bir parçası olmalıdır. Web uygulamalarına yönelik saldırıların büyük çoğunluğu, bilinen ve önlenebilir güvenlik açıklarından kaynaklanmaktadır. OWASP Top 10 gibi endüstri standartlarına atıfta bulunmak,

geliştiricilere somut ve denetlenebilir bir hedef listesi sunar . Bu, "güvenli kod yazın" gibi soyut bir ifadeden çok daha etkilidir. Politikanın bu standardı zorunlu kılması, geliştirme ekiplerine net bir yol haritası sunarken, BİDB'nin güvenlik denetimleri için de bir kontrol listesi görevi görür. Bu yaklaşım, güvenlik beklentilerini somutlaştırır, hesap verebilirliği artırır ve üniversitenin genel siber güvenlik duruşunu proaktif bir şekilde güçlendirir.

- BİDB sunucularında çalışacak tüm özel geliştirmeler ve uygulamalar, OWASP (Open Web Application Security Project) Top 10'da listelenen en kritik güvenlik risklerine karşı korunacak şekilde tasarlanmalı ve kodlanmalıdır.
- Uygulamalar, en az ayrıcalık (least privilege) ilkesine göre çalışmalı, veritabanı ve dosya sistemi erişimleri minimumda tutulmalıdır.
- Tüm kullanıcı girdileri (formlar, URL parametreleri vb.) sunucu tarafında doğrulanmalı ve temizlenmelidir (input validation/sanitization).
- BİDB, yeni web uygulamalarını yayına almadan önce veya periyodik olarak zafiyet taramasından geçirme hakkını saklı tutar. Tespit edilen kritik zafiyetler giderilmeden uygulama yayına alınamaz veya yayından kaldırılabilir.

6.3 E-Ticaret ve Ödeme Sistemleri İçin Özel Güvenlik Gereksinimleri

- Üniversite adına kredi kartı veya diğer elektronik ödeme yöntemleriyle tahsilat yapan tüm web siteleri, BİDB ve Mali İşler Daire Başkanlığı'ndan ön onay almak zorundadır.
- Bu tür siteler, PCI-DSS (Payment Card Industry Data Security Standard) uyumluluğunu sağlamakla yükümlüdür. Kredi kartı bilgilerinin üniversite sunucularında saklanması kesinlikle y asaktır. Ödeme işlemleri, PCI -DSS uyumlu üçüncü parti ödeme geçidi sağlayıcıları üzerinden gerçekleştirilmelidir.
- E-ticaret siteleri, düzenli olarak iç ve dış güvenlik denetimlerinden geçmek zorundadır.

6.4 Güvenlik İhlali ve Olay Yönetimi Prosedürü

- Herhangi bir web sitesinde güvenlik ihlali (hacklenme, veri sızıntısı vb.) şüphesi veya tespiti durumunda, Teknik Sorumlu derhal BİDB Güvenlik Birimi'ne (securityadmin@mail.ege.edu.tr) bildirimde bulunmalıdır.
- BİDB, ihlalin kapsamını belirlemek, zararı sınırlandırmak ve sistemi güvenli hale getirmek için ilgili web sitesine erişimi derhal askıya alabilir.
- Olay müdahale süreci, BİDB Siber Olaylara Müdahale Ekibi (SOME) tarafından yönetilir ve ilgili birimle koordinasyon içinde yürütülür.

Bölüm 7: Politika İhlalleri ve Yaptırımlar

Yürürlükte olan alan adı ve barındırma politikasını ihlal eden her türlü girişim ile ilgili olarak Üniversite bünyesinde faaliyet gösteren 1. dereceden sorumlu birim EBYS aracılığı ile bilgilendirilerek politika içeriğinde belirtilen yaptırımların belirtilen süreler geçerli olacak şekilde uygulanması sağlanacaktır.

7.1 İhlallerin Tespiti ve Raporlanması

Politika ihlalleri, BİDB'nin rutin denetimleri, otomatik güvenlik tarama sistemleri veya üçüncü şahıslardan gelen bildirimler (abuse@ege.edu.tr) yoluyla tespit edilebilir.

7.2 Uygulanacak Yaptırımlar

İhlalin niteliğine ve ciddiyetine bağlı olarak, BİDB aşağıdaki yaptırımları aşamalı olarak uygulama hakkını saklı tutar:

- **Seviye 1 (Uyarı):** Küçük çaplı ihlaller (örn: kurumsal kimliğe uymayan logo kullanımı, bozuk linkler) için Hizmet Sahibine ve Teknik Sorumluya yazılı bir uyarı gönderilir ve ihlalin belirli bir süre içinde (örn: 15 gün) düzeltilmesi istenir.
- **Seviye 2 (Hizmeti Askıya Alma):** Uyarılara rağmen düzeltilmeyen ihlaller, kritik güvenlik zafiyetleri veya Kabul Edilebilir Kullanım Politikasının ciddi ihlalleri durumunda, ilgili web sitesi veya hizmet, ihlal giderilene kadar geçici olarak erişime kapatılır.
- **Seviye 3 (Hizmeti Sonlandırma):** Yasa dışı faaliyetler, kasıtlı ve tekrarlayan ciddi ihlaller veya üniversitenin itibarına ve altyapısına büyük zarar veren durumlarda, alan adı ve barındırma hizmeti kalıcı olarak sonlandırılır.

Ayrıca, politika ihlali gerçekleştiren personel veya öğrenciler hakkında Üniversitenin ilgili Disiplin Yönetmelikleri uyarınca işlem başlatılabilir.

7.3 İtiraz Süreci ve Değerlendirme Kurulu

- Hizmet Sahibi, uygulanan yaptırımlara karşı, kararın tebliğinden itibaren yedi (7) iş günü içinde BİDB'ye EBYS üzerinden yazılı olarak itiraz edebilir.
- İtirazlar, BİDB Başkanlığı tarafından yeter sayıda temsilcinin oluşturduğu ilgili personeller tarafından incelenir ve karara bağlanır. Kurulun kararı nihaidir.