# RENKLİHOST KABUL EDİLEBİLİR KULLANIM POLİTİKASI (AUP)

**Son Güncelleme: 13 Eylül 2026**

## 1. AMAÇ

İşbu Kabul Edilebilir Kullanım Politikası (“AUP”), **CreaArt Teknoloji Anonim Şirketi – RENKLİHOST** tarafından sunulan hizmetlerin güvenli, hukuka uygun, sürdürülebilir ve diğer kullanıcıların haklarını ihlal etmeyecek şekilde kullanılmasına ilişkin kuralları belirlemektedir.

Bu Politikanın amacı;

- RENKLİHOST altyapısının güvenliğini korumak,
- müşterilerin ve üçüncü kişilerin haklarını korumak,
- kötüye kullanım faaliyetlerini önlemek,
- ağ ve IP itibarını korumak,
- spam, phishing, zararlı yazılım ve saldırı faaliyetleriyle mücadele etmek,
- ortak sistem kaynaklarının adil kullanımını sağlamak,
- yürürlükteki mevzuata uygun hizmet sunmak

olarak belirlenmiştir.

---

# 2. HİZMET SAĞLAYICI

**CreaArt Teknoloji Anonim Şirketi**
**Marka:** RENKLİHOST

**Adres:** Akademi Mah. Gürbulut Sk. S.Ü. Teknoloji Geliştirme Bölgesi, Konya Teknokent No:67, 42150 Selçuklu / Konya / Türkiye

**Vergi Dairesi:** Meram Vergi Dairesi Müdürlüğü
**Vergi No:** 2150650663
**MERSİS No:** 0215065066300001

**Telefon:** +90 850 307 3654
**E-posta:** info@renklihost.com
**Web:** www.renklihost.com

Bundan böyle **“RENKLİHOST”** olarak anılacaktır.

---

# 3. KAPSAM

İşbu Politika;

- Web Hosting,
- WordPress Hosting,
- E-posta Hosting,
- Reseller/Bayi Hosting,
- VPS/VDS,
- Cloud Sunucu,
- Dedicated/Fiziksel Sunucu,
- Oyun Sunucuları,
- Sunucu Barındırma,
- VPN hizmetleri,
- IP adresleri ve IP blokları,
- CDN,
- WAF,
- DDoS Koruma,
- Yedekleme,
- alan adı,
- SSL,
- lisans,
- diğer tüm dijital ve altyapı hizmetleri

dahil olmak üzere RENKLİHOST tarafından sağlanan hizmetlerin tamamında uygulanır.

MÜŞTERİ, RENKLİHOST hizmetlerini kullanmaya başlamasıyla işbu Politikaya uygun hareket etmekle yükümlüdür.

---

# 4. MÜŞTERİNİN GENEL SORUMLULUĞU

MÜŞTERİ;

kendi hesabı,

hosting alanı,

sunucusu,

IP adresi,

alan adı,

uygulamaları,

kullanıcıları,

bayi hesapları,

API anahtarları

üzerinden gerçekleştirilen faaliyetlerden sorumludur.

MÜŞTERİ hizmetlerini üçüncü kişilere kullandırıyorsa bu kişilerin de işbu Politikaya uygun hareket etmesini sağlamakla yükümlüdür.

Bir faaliyetin MÜŞTERİ tarafından doğrudan yapılmamış olması, MÜŞTERİ'nin sisteminin ele geçirilmiş veya kötü amaçlı yazılım bulaşmış olması halinde dahi güvenlik tehdidinin giderilmesi için RENKLİHOST'un gerekli teknik tedbirleri almasına engel değildir.

---

# 5. HUKUKA UYGUN KULLANIM

RENKLİHOST hizmetleri yürürlükteki mevzuata uygun şekilde kullanılmalıdır.

Hizmetlerin;

suç işlemek,

suç işlenmesini kolaylaştırmak,

hukuka aykırı içerik yayınlamak,

hukuka aykırı verilerin dağıtımını gerçekleştirmek,

başkalarının haklarını ihlal etmek

amacıyla kullanılması yasaktır.

MÜŞTERİ, faaliyetinin niteliğine göre Türkiye Cumhuriyeti mevzuatına ve uygulanması zorunlu diğer mevzuata uymakla yükümlüdür.

---

# 6. KESİNLİKLE YASAKLANAN FAALİYETLER

Aşağıdaki faaliyetler RENKLİHOST altyapısında kesinlikle yasaktır:

- phishing ve kimlik avı,
- finansal dolandırıcılık,
- sahte banka veya ödeme sayfaları,
- kart bilgilerinin hukuka aykırı şekilde elde edilmesi,
- malware dağıtımı,
- ransomware,
- trojan,

- botnet,
- credential stealer,
- keylogger,
- hukuka aykırı uzaktan erişim yazılımları,
- yetkisiz kripto madenciliği yazılımları,
- başkasının sistemine izinsiz erişim,
- DDoS/DoS saldırısı,
- saldırı altyapısı barındırılması,
- spam gönderimi,
- hukuka aykırı toplu mesaj faaliyetleri,
- çocukların cinsel istismarıyla bağlantılı içerikler,
- dolandırıcılık ve sahtecilik,
- yasa dışı ürün veya hizmetlerin satışı,
- yürürlükteki mevzuat kapsamında suç oluşturan diğer faaliyetler.

RENKLİHOST bu tür faaliyetlerde hizmeti önceden bildirim yapmaksızın askıya alabilir.

---

# 7. ÇOCUKLARIN CİNSEL İSTİSMARINA İLİŞKİN İÇERİKLER

Çocukların cinsel istismarına ilişkin görüntü, video, dosya, bağlantı, materyal veya bunların dağıtımını kolaylaştıran içeriklerin RENKLİHOST altyapısında barındırılması kesinlikle yasaktır.

Bu tür bir durumun güvenilir şekilde tespit edilmesi halinde RENKLİHOST;

ilgili hizmeti derhal askıya alabilir,

erişimi engelleyebilir,

ilgili kayıtları koruma altına alabilir

ve yürürlükteki mevzuat kapsamında yetkili makamlarla iş birliği yapabilir.

---

# 8. PHISHING VE KİMLİK AVI

Başka kişi veya kuruluşların;

banka,

ödeme kuruluşu,

e-ticaret sitesi,

sosyal medya,

e-posta,

kripto platformu,

kamu kurumu,

şirket veya marka

gibi görünmesini sağlayarak kullanıcı adı, parola, kart bilgisi veya diğer hassas bilgilerin elde edilmeye çalışılması yasaktır.

Phishing tespit edilen hizmetler acil güvenlik tehdidi olarak değerlendirilebilir.

---

# 9. ZARARLI YAZILIM

RENKLİHOST hizmetleri;

virüs,

trojan,

ransomware,

keylogger,

credential stealer,

worm,

rootkit,

bot,

backdoor

gibi zararlı yazılımların oluşturulması, barındırılması veya dağıtılması için kullanılamaz.

Meşru güvenlik araştırmaları ancak sistem sahibinin izni ve uygulanabilir hukuka uygun şekilde gerçekleştirilebilir.

---

# 10. BOTNET FAALİYETLERİ

Botnet;

komuta-kontrol sunucusu,

zararlı yazılım dağıtım noktası,

bot yönetim paneli,

ele geçirilmiş cihaz yönetimi

amacıyla RENKLİHOST altyapısının kullanılması yasaktır.

Tespit edilen botnet altyapısı önceden uyarı yapılmadan devre dışı bırakılabilir.

---

# 11. DDoS VE DoS SALDIRILARI

RENKLİHOST hizmetlerinin başka bir sistem veya kullanıcıya yönelik;

DDoS,

DoS,

UDP flood,

SYN flood,

HTTP flood,

amplification,

reflection

ve benzeri saldırılarda kullanılması yasaktır.

Ayrıca DNS, NTP, SSDP, memcached ve benzeri servislerin kötüye kullanıma açık amplification/reflection kaynağı olacak şekilde yapılandırılması yasaktır.

---

# 12. PORT TARAMA VE GÜVENLİK TARAMALARI

MÜŞTERİ'nin sahibi olmadığı veya test için açık izin almadığı sistemler üzerinde;

port taraması,

zafiyet taraması,

brute-force,

credential stuffing,

exploit denemeleri,

otomatik güvenlik saldırıları

gerçekleştirmesi yasaktır.

MÜŞTERİ kendi sisteminde veya açık yetki aldığı sistemlerde hukuka uygun güvenlik testi gerçekleştirebilir.

Ancak gerçekleştirilen testin RENKLİHOST ağına veya üçüncü kişilere zarar vermemesi gerekir.

---

# 13. BRUTE-FORCE VE CREDENTIAL STUFFING

SSH,

RDP,

FTP,

SMTP,

WordPress,

e-posta,

kontrol paneli

ve diğer servislerde yetkisiz hesap erişimi sağlamak amacıyla parola denemeleri yapılması yasaktır.

Bu faaliyetlerin gerçekleştiği IP adresleri otomatik olarak engellenebilir veya ilgili hizmet geçici olarak izole edilebilir.

---

# 14. SPAM

İstenmeyen toplu elektronik posta gönderimi yasaktır.

MÜŞTERİ;

izin alınmamış adres listelerine toplu e-posta gönderemez,

satın alınmış veya hukuka aykırı şekilde elde edilmiş e-posta listelerini kullanamaz,

spam faaliyetlerinin yönlendirildiği landing page veya internet sitesini RENKLİHOST üzerinde barındıramaz,

üçüncü taraf sistemler üzerinden spam gönderip RENKLİHOST altyapısındaki siteye trafik yönlendiremez.

Spam yalnızca mesajın RENKLİHOST sunucusundan çıkmasıyla sınırlı değerlendirilmez.

---

# 15. E-POSTA GÖNDERİM KURALLARI

Toplu e-posta gönderimi gerçekleştirilen sistemlerde MÜŞTERİ;

gerekli ticari ileti izinlerini almak,

geçerli gönderici bilgisi kullanmak,

çalışan abonelikten çıkma mekanizması sağlamak,

bounce ve şikâyet oranlarını kontrol etmek,

spam tuzağı veya satın alınmış liste kullanmamak

zorundadır.

Paylaşımlı hosting ve e-posta hizmetlerinde saatlik gönderim, alıcı sayısı, mailbox kapasitesi ve benzeri teknik sınırlar paket özelliklerine göre uygulanabilir.

Güncel teknik limitler ilgili ürün sayfası, müşteri paneli veya RENKLİHOST tarafından bildirilen teknik limitler üzerinden belirlenir.

---

# 16. IP İTİBARI VE BLACKLIST

MÜŞTERİ'nin faaliyetleri nedeniyle RENKLİHOST'a ait IP adreslerinin;

spam blacklist,

RBL,

DNSBL,

e-posta itibar sistemi,

güvenlik engelleme listesi

üzerinde listelenmesine neden olunması yasaktır.

IP itibarına zarar veren hizmetler geçici olarak durdurulabilir.

RENKLİHOST gerekli gördüğünde ilgili portları veya protokolleri geçici olarak kısıtlayabilir.

---

# 17. SMTP / PORT 25 KISITLAMALARI

RENKLİHOST, spam ve kötüye kullanımı önlemek amacıyla özellikle yeni veya riskli sunucularda SMTP/25 çıkış trafiğini varsayılan olarak kısıtlayabilir.

MÜŞTERİ, meşru e-posta gönderim ihtiyacının bulunması halinde gerekli doğrulamaları sağlayarak kısıtlamanın kaldırılmasını talep edebilir.

RENKLİHOST güvenlik ve IP itibarı nedeniyle bu talebi kabul etmeme hakkını saklı tutar.

---

# 18. OPEN RELAY VE AÇIK PROXY

Yetkisiz kişilerin kullanabileceği;

open mail relay,

açık HTTP/SOCKS proxy,

kötüye kullanıma açık DNS resolver,

açık NTP amplification servisi

gibi sistemlerin çalıştırılması yasaktır.

Güvenlik açığı nedeniyle istemeden bu hale gelen hizmetlerde MÜŞTERİ'den sorunu gidermesi istenebilir veya hizmet geçici olarak izole edilebilir.

---

# 19. VPN HİZMETLERİ

RENKLİHOST tarafından VPN kullanımına uygun olarak satılan ürünlerde VPN hizmeti çalıştırılabilir.

VPN teknolojisinin kendisi yasak değildir.

Ancak VPN;

siber saldırı,

spam,

phishing,

dolandırıcılık,

telif ihlali,

yetkisiz sistem erişimi,

diğer yasa dışı faaliyetlerin

gizlenmesi veya gerçekleştirilmesi amacıyla kullanılamaz.

Herkese açık ve kontrolsüz proxy/VPN servisi işletilmesi RENKLİHOST'un önceden yazılı iznine tabi tutulabilir.

---

# 20. TOR VE ANONİMLEŞTİRME SERVİSLERİ

Tor relay veya benzeri anonimleştirme teknolojilerinin kullanımı hizmet türüne göre değerlendirilebilir.

**Tor Exit Node**, kötüye kullanım riskinin yüksek olması nedeniyle RENKLİHOST'un önceden yazılı izni olmaksızın çalıştırılamaz.

RENKLİHOST, abuse bildirimlerinin yoğunlaşması halinde anonimleştirme hizmetlerini kısıtlayabilir.

---

# 21. KRİPTO PARA MADENCİLİĞİ

Paylaşımlı hosting, reseller ve e-posta hizmetlerinde kripto para madenciliği kesinlikle yasaktır.

VPS/VDS veya fiziksel sunucularda kripto madenciliğine ancak ilgili ürünün kullanım şartlarında açıkça izin verilmesi halinde müsaade edilebilir.

Kaynak kullanımını gizlemek amacıyla madencilik yazılımı çalıştırılması veya ele geçirilmiş sistemlerde madencilik yapılması kesinlikle yasaktır.

---

# 22. KRİPTO PARA VE BLOCKCHAIN HİZMETLERİ

Blockchain node, wallet servisleri ve hukuka uygun diğer blockchain uygulamaları kullanılan hizmet türüne göre barındırılabilir.

Bununla birlikte;

kripto dolandırıcılığı,

sahte yatırım sitesi,

seed phrase veya private key hırsızlığı,

phishing,

ponzi/piramit yapıları,

zararlı kripto uygulamaları

yasaktır.

---

# 23. DOSYA PAYLAŞIMI VE TORRENT

Paylaşımlı hosting hizmetleri;

torrent seedbox,

genel amaçlı dosya paylaşım platformu,

dosya depolama sunucusu,

yüksek trafikli download mirror

olarak kullanılamaz; ilgili ürün özelliklerinde aksi açıkça belirtilmiş olması hali saklıdır.

VPS/VDS ve dedicated hizmetlerde dosya paylaşımı ancak hukuka uygun içerik için ve ilgili ürünün ağ/kaynak limitlerine uygun şekilde gerçekleştirilebilir.

Telif hakkını ihlal eden içeriklerin dağıtılması yasaktır.

---

# 24. SÜREKLİ DOWNLOAD / UPLOAD VE AĞ KULLANIMI

RENKLİHOST'un belirli sunucu hizmetlerinde trafik miktarı veya port kapasitesi belirtilmiş olabilir.

MÜŞTERİ'nin ağ kullanımının;

diğer müşterilerin hizmet kalitesini bozması,

ağ altyapısını olağandışı yük altında bırakması,

ürünün tasarlanan kullanım amacını aşması

halinde RENKLİHOST trafik şekillendirmesi, rate-limit veya geçici kısıtlama uygulayabilir.

Sınırsız trafik olarak belirtilen hizmetler, teknik olarak limitsiz kaynak garantisi anlamına gelmez; hizmetin niteliğine göre makul kullanım ve port kapasitesi sınırları uygulanabilir.

---

# 25. PAYLAŞIMLI HOSTING KAYNAK KULLANIMI

Paylaşımlı hosting altyapısında;

CPU,

RAM,

disk I/O,

IOPS,

process,

inode,

MySQL,

eş zamanlı bağlantı,

e-posta

gibi kaynaklar diğer kullanıcılarla paylaşılır.

Bir hesabın diğer kullanıcıların hizmet kalitesini ciddi şekilde etkileyecek seviyede sürekli kaynak tüketmesi halinde;

kaynak kısıtlaması,

geçici askıya alma,

paket yükseltme talebi,

VPS/VDS'ye geçiş önerisi

uygulanabilir.

Teknik limitler ürün özelliklerinde veya müşteri panelinde belirtilen güncel değerler üzerinden uygulanır.

---

# 26. SINIRSIZ KAYNAK İFADESİ

Bir hizmette;

“sınırsız trafik”,

“sınırsız web sitesi”,

“sınırsız e-posta”

gibi bir ifade bulunması, fiziksel olarak sınırsız CPU, RAM, disk performansı veya ağ kapasitesi sağlandığı anlamına gelmez.

Kullanım;

paketin teknik özellikleri,

altyapının fiziksel kapasitesi,

adil kullanım,

diğer müşterilerin hizmet kalitesi

çerçevesinde değerlendirilir.

---

# 27. DEPOLAMA ALANININ KÖTÜYE KULLANIMI

Web hosting paketlerindeki disk alanı öncelikle ilgili internet sitesinin çalışması için kullanılmalıdır.

Paylaşımlı web hosting hesapları, aksi açıkça belirtilmedikçe;

kişisel bulut depolama,

genel dosya arşivi,

yedek deposu,

video arşivi,

disk mirror,

torrent deposu

olarak kullanılamaz.

RENKLİHOST ayrıca ayrı yedekleme veya depolama hizmetleri sunabilir.

---

# 28. VERİTABANI KULLANIMI

Paylaşımlı hosting üzerinde sağlanan MySQL veya diğer veritabanı hizmetleri ilgili hosting hesabının çalışması amacıyla sunulur.

RENKLİHOST güvenlik veya performans nedeniyle;

uzak veritabanı erişimini,

eş zamanlı bağlantı sayısını,

sorgu süresini,

kaynak kullanımını

sınırlandırabilir.

Güncel teknik limitler ilgili hizmet planına göre belirlenir.

---

# 29. BAĞIMSIZ VE SÜREKLİ SERVER-SIDE İŞLEMLER

Paylaşımlı hosting hizmetlerinde web barındırma amacının dışında;

daemon,

IRC server,

arka planda sürekli çalışan bot,

sürekli crawler,

proxy,

oyun sunucusu,

yüksek kaynak kullanan worker

gibi bağımsız servisler çalıştırılamaz.

Bu tip uygulamalar için uygun VPS/VDS veya dedicated hizmet kullanılmalıdır.

---

# 30. CRON VE OTOMASYON GÖREVLERİ

Paylaşımlı hosting hesaplarında aşırı sıklıkta çalışan;

cron,

queue worker,

crawler,

import/export,

API görevi

gibi işlemler diğer kullanıcıları etkilemeyecek şekilde kullanılmalıdır.

RENKLİHOST gerektiğinde minimum çalışma aralığı veya kaynak limiti uygulayabilir.

---

# 31. OYUN SUNUCULARI

RENKLİHOST tarafından oyun sunucusu amacıyla sağlanan hizmetlerde;

Minecraft,

FiveM,

Counter-Strike,

Rust

ve benzeri oyun sunucuları çalıştırılabilir.

MÜŞTERİ;

oyun üreticisinin kullanım koşullarına,

uygulanabilir lisans şartlarına,

işbu AUP'ye

uymakla yükümlüdür.

Oyun sunucusunun DDoS saldırısı gerçekleştirmek, malware dağıtmak veya başka hizmetlere saldırmak için kullanılması yasaktır.

---

# 32. FIVE M VE MOD İÇERİKLERİ

FiveM veya diğer modlanabilir oyun sunucularında kullanılan;

script,

mod,

model,

müzik,

harita,

yazılım

gibi içeriklerin kullanım haklarının sağlanması MÜŞTERİ'nin sorumluluğundadır.

RENKLİHOST müşterinin yüklediği üçüncü taraf içeriklerin lisans sahibi olduğunu garanti etmez.

---

# 33. FİKRİ MÜLKİYET VE TELİF HAKLARI

MÜŞTERİ;

telif hakkı,

marka hakkı,

patent,

tasarım,

lisans

ve diğer fikri veya sınai mülkiyet haklarını hukuka aykırı şekilde ihlal eden içerikleri barındıramaz veya dağıtamaz.

Hak sahibi tarafından yeterli bilgi ve belge içeren bir ihlal bildirimi gönderilmesi halinde RENKLİHOST bildirimi inceleyebilir ve gerekli durumlarda MÜŞTERİ'den açıklama veya içeriğin kaldırılmasını isteyebilir.

---

# 34. SAHTE ÜRÜN VE MARKA TAKLİDİ

Başka bir markayı veya işletmeyi taklit ederek;

sahte ürün satışı,

dolandırıcılık,

kimlik avı,

müşteri yanıltma

amacıyla hizmet kullanılması yasaktır.

---

# 35. KİŞİSEL VERİLERİN HUKUKA AYKIRI KULLANIMI

Hizmetlerin;

çalınmış kişisel veri,

hukuka aykırı elde edilmiş müşteri listesi,

çalınmış hesap bilgileri,

kart verileri,

şifre veri tabanları

gibi verilerin barındırılması veya dağıtılması amacıyla kullanılması yasaktır.

MÜŞTERİ kendi internet sitesi veya uygulamasında işlediği kişisel veriler bakımından yürürlükteki veri koruma mevzuatına uymakla yükümlüdür.

---

# 36. YANILTICI VE DOLANDIRICI İÇERİKLER

Hizmetlerin;

sahte yatırım sitesi,

sahte kampanya,

sahte çekiliş,

sahte ödeme sitesi,

sahte destek hattı,

kimlik hırsızlığı,

kullanıcıları yanıltmaya yönelik finansal sistemler

için kullanılması yasaktır.

---

# 37. KAYNAK TÜKETİMİNİ GİZLEME

MÜŞTERİ'nin;

kaynak limitlerini aşmak,

trafik limitlerini atlatmak,

kullanım ölçümünü engellemek,

güvenlik sistemlerini yanıltmak

amacıyla teknik yöntem kullanması yasaktır.

---

# 38. SANALLAŞTIRMA VE NESTED VIRTUALIZATION

VPS/VDS hizmetlerinde nested virtualization veya ek sanallaştırma teknolojileri yalnızca teknik altyapının desteklediği ve ürün şartlarında izin verildiği durumlarda kullanılabilir.

RENKLİHOST, altyapı kararlılığını etkileyen sanallaştırma faaliyetlerini kısıtlayabilir.

---

# 39. IP SPOOFING

Kaynak IP adresinin sahte gösterilmesi veya RENKLİHOST ağı üzerinden IP spoofing gerçekleştirilmesi yasaktır.

RENKLİHOST ağ güvenliği kapsamında spoof edilmiş trafiği filtreleyebilir.

---

# 40. MAC / ARP / DHCP KÖTÜYE KULLANIMI

Sunucu barındırma ve fiziksel altyapı hizmetlerinde;

yetkisiz IP kullanımı,

ARP spoofing,

DHCP spoofing,

başka müşteriye tahsisli IP adresini kullanma

yasaktır.

Yalnızca RENKLİHOST tarafından ilgili hizmete tahsis edilen IP adresleri kullanılmalıdır.

---

# 41. IP ADRESLERİNİN KULLANIMI

MÜŞTERİ'ye tahsis edilen IP adresleri mülkiyet devri anlamına gelmez.

IP adresleri hizmet süresince kullanım amacıyla tahsis edilir.

RENKLİHOST;

ağ değişikliği,

RIR/LIR politikaları,

güvenlik,

teknik zorunluluk

nedeniyle gerekli olduğunda IP adresini değiştirebilir.

Mümkün olduğu durumlarda MÜŞTERİ önceden bilgilendirilir.

---

# 42. DDoS KORUMA HİZMETİ

DDoS koruması, saldırının etkisini azaltmayı amaçlayan teknik bir hizmettir ve tüm saldırıların hiçbir koşulda etkisiz hale getirileceği anlamına gelmez.

Bir hizmetin aldığı saldırının diğer müşterileri veya genel ağı ciddi şekilde etkilemesi halinde RENKLİHOST;

blackhole,

null-route,

rate-limit,

geçici trafik engeli

uygulayabilir.

---

# 43. AĞ GÜVENLİĞİ

MÜŞTERİ;

sunucusunda gereksiz servisleri kapatmak,

güçlü parola kullanmak,

yazılımları güncel tutmak,

güvenlik açıklarını gidermek

için makul tedbirleri almakla yükümlüdür.

Ele geçirilmiş veya saldırı kaynağı haline gelmiş sistemler, ağın ve üçüncü kişilerin güvenliği için geçici olarak izole edilebilir.

---

# 44. GÜVENLİK AÇIĞI BULUNAN SİSTEMLER

RENKLİHOST bir MÜŞTERİ sisteminin;

botnet parçası,

spam kaynağı,

açık proxy,

amplification kaynağı,

malware dağıtım noktası

haline geldiğini tespit ederse MÜŞTERİ'den güvenlik sorununu gidermesini isteyebilir.

Acil risk bulunuyorsa hizmet önceden bildirim yapılmadan geçici olarak kısıtlanabilir.

---

# 45. ABUSE BİLDİRİMLERİ

RENKLİHOST altyapısında barındırılan bir hizmet hakkında;

phishing,

spam,

malware,

telif,

dolandırıcılık,

siber saldırı,

hukuka aykırı içerik

şikâyetleri alınabilir.

Abuse bildiriminin mümkün olduğu ölçüde;

ilgili IP veya alan adını,

şikâyete konu URL'yi,

olayın tarih ve saatini,

teknik logları,

şikâyetin açıklamasını,

varsa hukuki hak sahipliğini gösteren bilgileri

içermesi beklenir.

---

# 46. ABUSE BİLDİRİMLERİNİN İNCELENMESİ

RENKLİHOST her abuse bildirimini doğrudan doğru kabul etmek zorunda değildir.

Bildirim;

güvenilirliği,

teknik delilleri,

hukuki niteliği,

aciliyeti,

üçüncü kişilere yönelik riski

bakımından değerlendirilebilir.

Açıkça kötü niyetli veya delilsiz bildirimler reddedilebilir.

---

# 47. MÜŞTERİYE BİLDİRİM

Acil risk bulunmayan ihlallerde RENKLİHOST MÜŞTERİ'ye durumu bildirerek ihlalin giderilmesi için makul süre verebilir.

Sürenin uzunluğu;

ihlalin niteliğine,

riskin seviyesine,

üçüncü kişilere verilen zarara

göre belirlenir.

---

# 48. DERHAL MÜDAHALE EDİLEBİLECEK DURUMLAR

Aşağıdaki hallerde RENKLİHOST önceden bildirim yapmadan hizmeti kısıtlayabilir veya askıya alabilir:

- phishing,
- aktif malware dağıtımı,
- DDoS saldırısı,
- botnet,
- ciddi spam saldırısı,
- dolandırıcılık,
- çocukların cinsel istismarına ilişkin içerik,
- üçüncü kişilerin sistemlerine aktif saldırı,
- RENKLİHOST altyapısına ciddi güvenlik tehdidi,
- yetkili makamın uygulanması zorunlu kararı,
- diğer müşterilere ciddi zarar verme riski.

Bu müdahaleler öncelikle tehdidi durdurmak amacıyla gerçekleştirilir.

---

# 49. KADEMELİ YAPTIRIM

İhlalin niteliğine göre RENKLİHOST;

uyarı,

teknik kısıtlama,

port engelleme,

rate-limit,

IP bloklama,

servis izolasyonu,

geçici askıya alma,

kalıcı hizmet sonlandırma

tedbirlerinden bir veya birkaçını uygulayabilir.

Tedbir mümkün olduğu ölçüde ihlalin ağırlığıyla orantılı olarak uygulanır.

---

# 50. TEKRARLAYAN İHLALLER

Aynı MÜŞTERİ'nin veya hizmetin sürekli olarak abuse bildirimi alması veya daha önce giderilmesi istenen ihlalin tekrarlanması halinde RENKLİHOST daha ağır tedbirler uygulayabilir.

Tekrarlayan ciddi ihlaller sözleşmenin feshedilmesine neden olabilir.

---

# 51. HİZMETİN ASKIYA ALINMASI

Hizmet askıya alındığında;

internet erişimi,

web sitesi,

e-posta,

sunucu,

IP adresi,

müşteri hizmeti

kısmen veya tamamen erişilemez hale gelebilir.

Askıya alma, güvenlik sorunu giderildiğinde ve RENKLİHOST tarafından gerekli kontroller gerçekleştirildiğinde kaldırılabilir.

---

# 52. VERİYE ERİŞİM

Bir hizmetin AUP ihlali nedeniyle askıya alınması, MÜŞTERİ'ye her durumda hizmet içerisindeki verilere erişim garantisi verildiği anlamına gelmez.

Ancak güvenlik ve hukuki koşullar izin verdiği ölçüde RENKLİHOST MÜŞTERİ'nin verilerini almasına imkân sağlayabilir.

Acil saldırı, kötü amaçlı yazılım veya hukuki engel bulunması halinde erişim kısıtlanabilir.

---

# 53. HİZMETİN FESHİ

Ağır veya tekrarlanan AUP ihlallerinde RENKLİHOST ilgili hizmeti veya müşteri hesabını feshedebilir.

Özellikle;

phishing,

botnet,

aktif saldırı,

dolandırıcılık,

çocuk istismarı içeriği,

kasıtlı malware dağıtımı,

sürekli spam

gibi ağır ihlaller sözleşmenin derhal feshedilmesine neden olabilir.

---

# 54. İADE

AUP ihlali nedeniyle hizmetin kapatılması veya feshedilmesi halinde RENKLİHOST tarafından sunulan gönüllü/ticari para iade garantisi uygulanmayabilir.

Ancak tüketici sıfatındaki MÜŞTERİ'nin emredici mevzuattan doğan ve sözleşmeyle kaldırılamayan hakları saklıdır.

---

# 55. DELİL VE TEKNİK KAYITLAR

RENKLİHOST;

IP kayıtlarını,

ağ akış bilgilerini,

güvenlik loglarını,

e-posta gönderim kayıtlarını,

abuse bildirimlerini,

müşteri destek yazışmalarını,

hizmet aktivasyon kayıtlarını

güvenlik olaylarının ve uyuşmazlıkların araştırılması için mevzuata uygun şekilde saklayabilir.

Kişisel verilerin işlenmesi ayrıca RENKLİHOST KVKK Aydınlatma Metni ve Gizlilik Politikası kapsamında gerçekleştirilir.

---

# 56. RESMÎ MAKAMLAR

RENKLİHOST, hukuken yetkili kurum veya makamdan usulüne uygun bir talep gelmesi halinde yürürlükteki mevzuat kapsamında gerekli işlemleri gerçekleştirebilir.

Mahkeme, Cumhuriyet başsavcılığı, kolluk birimleri, Bilgi Teknolojileri ve İletişim Kurumu veya diğer yetkili makamların uygulanması zorunlu kararları doğrultusunda;

erişim kısıtlanabilir,

hizmet askıya alınabilir,

ilgili kayıtlar korunabilir veya paylaşılabilir.

---

# 57. BAYİ / RESELLER MÜŞTERİLER

Reseller/Bayi Hosting hizmeti kullanan MÜŞTERİ, kendi alt müşterilerinin işbu AUP'ye uygun hareket etmesini sağlamakla yükümlüdür.

Alt müşteri tarafından gerçekleştirilen bir ihlal, ilgili reseller hesabı bakımından da değerlendirmeye alınabilir.

RENKLİHOST ciddi güvenlik riskinde ilgili alt hesabı veya gerekli olması halinde bayi hesabını geçici olarak askıya alabilir.

---

# 58. SUNUCU BARINDIRMA HİZMETLERİ

MÜŞTERİ'ye ait fiziksel cihazın RENKLİHOST veya RENKLİHOST'un hizmet aldığı veri merkezinde barındırılması, cihazda gerçekleştirilen faaliyetlerin AUP dışında olduğu anlamına gelmez.

Barındırılan fiziksel cihazlar da işbu Politikaya tabidir.

---

# 59. MÜŞTERİNİN GÜVENLİK SORUMLULUĞU

Yönetimsiz VPS/VDS ve dedicated sunucularda;

işletim sistemi güvenliği,

yazılım güncellemeleri,

firewall,

kullanıcı hesapları,

SSH/RDP güvenliği,

web uygulamalarının güvenliği

kural olarak MÜŞTERİ'nin sorumluluğundadır.

RENKLİHOST'un saldırı tespit etmesi, MÜŞTERİ adına sunucu güvenliğini sürekli yönetme yükümlülüğü bulunduğu anlamına gelmez.

---

# 60. YÖNETİMLİ SUNUCULAR

MÜŞTERİ ayrıca yönetimli sunucu hizmeti satın almışsa RENKLİHOST'un güvenlik ve yönetim sorumlulukları satın alınan yönetim paketinin kapsamıyla sınırlıdır.

AUP hükümleri yönetimli sunucular için de geçerlidir.

---

# 61. KULLANIM LİMİTLERİ

RENKLİHOST hizmetlerin teknik kullanım limitlerini;

ürün sayfasında,

müşteri panelinde,

bilgi bankasında,

hizmete özel teknik dokümanda

belirtebilir.

Teknik altyapının gelişmesi nedeniyle bu limitlerin değişmesi gerekebilir.

Ön ödemesi yapılmış hizmetin temel özelliklerini esaslı şekilde değiştiren düzenlemelerde müşterinin sözleşmeden doğan hakları saklıdır.

---

# 62. MEVCUT TEKNİK LİMİTLERLE AUP ARASINDAKİ İLİŞKİ

Belirli paketlerde;

e-posta gönderim limiti,

mailbox kapasitesi,

eş zamanlı veritabanı bağlantısı,

CPU/RAM limiti,

disk I/O,

inode,

trafik,

port kapasitesi

gibi teknik sınırlar ayrıca uygulanabilir.

İlgili hizmet için açıkça tanımlanan paket limitleri işbu AUP'nin tamamlayıcı parçasıdır.

---

# 63. YANLIŞ POZİTİF VE İTİRAZ

Bir hizmetin yanlışlıkla AUP ihlali olarak değerlendirildiğini düşünen MÜŞTERİ, müşteri paneli üzerinden destek talebi oluşturarak inceleme talep edebilir.

RENKLİHOST mümkün olduğu ölçüde teknik kayıtları yeniden değerlendirir.

İhlalin bulunmadığının anlaşılması halinde uygulanan kısıtlama kaldırılabilir.

---

# 64. ACİL GÜVENLİK ÖNCELİĞİ

RENKLİHOST'un bir güvenlik olayında önceliği;

aktif tehdidi durdurmak,

diğer müşterileri korumak,

ağ güvenliğini sağlamak,

zararın büyümesini engellemektir.

Bu nedenle acil durumlarda inceleme tamamlanmadan geçici önleyici tedbir uygulanabilir.

---

# 65. ÜÇÜNCÜ TARAF SAĞLAYICI KURALLARI

RENKLİHOST'un hizmet verirken kullandığı;

veri merkezi,

network operatörü,

IP sağlayıcısı,

domain registrar,

lisans sağlayıcısı,

upstream provider

tarafından uygulanan hukuka uygun kullanım ve abuse kuralları ilgili hizmetlerde ayrıca uygulanabilir.

MÜŞTERİ'nin faaliyeti RENKLİHOST'un upstream sağlayıcısının ağı bakımından ciddi risk oluşturuyorsa gerekli teknik tedbir alınabilir.

---

# 66. POLİTİKANIN KÖTÜYE KULLANILMAMASI

İşbu AUP;

meşru eleştiri,

hukuka uygun ifade özgürlüğü,

meşru güvenlik araştırması,

yasal ticari faaliyet

gibi faaliyetlerin keyfi biçimde engellenmesi amacıyla kullanılmaz.

Bir içeriğin yalnızca tartışmalı, eleştirel veya rahatsız edici olması tek başına teknik hizmetin kapatılması için yeterli olmayabilir.

Hukuki veya ciddi güvenlik riski değerlendirmesi olayın niteliğine göre yapılır.

---

# 67. AUP İLE DİĞER SÖZLEŞMELERİN İLİŞKİSİ

İşbu Kabul Edilebilir Kullanım Politikası;

**RENKLİHOST Hizmet Sözleşmesi,**

**Mesafeli Satış Sözleşmesi,**

**İptal ve İade Koşulları,**

**Gizlilik ve Güvenlik Politikası,**

**Çerez Politikası,**

**KVKK Aydınlatma Metni**

ve ilgili hizmete özel koşullarla birlikte uygulanır.

---

# 68. POLİTİKA DEĞİŞİKLİKLERİ

RENKLİHOST;

yeni güvenlik tehditleri,

teknolojik gelişmeler,

altyapı değişiklikleri,

upstream sağlayıcı gereksinimleri,

mevzuat değişiklikleri

nedeniyle işbu Politikayı güncelleyebilir.

Güncel sürüm www.renklihost.com üzerinden yayımlanır.

Mevcut müşterilerin haklarını esaslı şekilde etkileyen değişikliklerde mümkün olduğu ölçüde ayrıca bildirim yapılabilir.

---

# 69. ABUSE VE GÜVENLİK İLETİŞİMİ

RENKLİHOST altyapısından kaynaklanan;

spam,

phishing,

malware,

siber saldırı,

telif ihlali,

dolandırıcılık

ve diğer kötüye kullanım bildirimleri için RENKLİHOST ile iletişime geçilebilir.

**E-posta:** info@renklihost.com
**Müşteri Paneli:** www.renklihost.com
**Telefon:** +90 850 307 3654

RENKLİHOST ilerleyen dönemde abuse bildirimleri için ayrı bir e-posta adresi ilan edebilir.

---

# 70. YÜRÜRLÜK

İşbu **RenkliHost Kabul Edilebilir Kullanım Politikası (AUP)**, **13 Eylül 2026** tarihinde güncellenmiş olup www.renklihost.com üzerinden yayımlandığı tarihten itibaren yürürlüğe girer.

MÜŞTERİ, RENKLİHOST hizmetlerini kullanırken işbu Politikaya uygun hareket etmekle yükümlüdür.

**CREART TEKNOLOJİ ANONİM ŞİRKETİ – RENKLİHOST**

Akademi Mah. Gürbulut Sk. S.Ü. Teknoloji Geliştirme Bölgesi
Konya Teknokent No:67
42150 Selçuklu / Konya / Türkiye

**VKN:** 2150650663
**MERSİS No:** 0215065066300001
**E-posta:** info@renklihost.com
**Telefon:** +90 850 307 3654
**Web:** www.renklihost.com