1. **AMAÇ:**

Bilgi Güvenliği Yönetim Sistemi (BGYS) Politikalarının amacı; Karabük Üniversitesi çalışanlarının, sistemlerinin, bilgi ve varlıklarının; gizlilik, bütünlük ve erişilebilirlik bakımından yapılması, uyulması gereken iş kurallarını hedeflemek ve bu hedefler kapsamında iş sürekliliğini sağlamaktır.

Kurumun amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Kurum bilerek / bilmeyerek yapılan, yasadışı veya zararlı eylemlere karşı çalışanın ve kurumun haklarını koruma altına almaktadır. Bilgi teknolojileri ile alakalı sistemler kurumun sahip olduğu değerlerdir. Güçlü bir bilgi güvenliği tüm çalışanların dâhil olduğu takım çalışmasıyla gerçekleştirilir. Bilgi güvenliğinin sağlanabilmesi için tüm personelin bilgi güvenliği politikalarını iyi bilmesi ve uygulamanın sorumluluğunu taşıyabilmesi gerekmektedir.

1. **KAPSAM:**

Bilgi Güvenliği Yönetim Sistemi dâhilinde yapılan işlemler.

1. **YAPTIRIM:**

Bu politikalara uygun olarak hareket etmeyen personel hakkında 2547 sayılı Yükseköğretim Kanunu ve 657 sayılı Devlet Memurları Kanunu’nun disiplin ve ceza işlerine ilişkin hükümleri, öğrenciler hakkında Yükseköğretim Kurumları Öğrenci Disiplin Yönetmeliği uygulanacak, disiplin işlemlerinin yanı sıra eylemin niteliğine uygun olarak ilgili mevzuat hükümleri uyarınca yasal işlem yapılacaktır. Tedarikçi ve ziyaretçiler için ise genel hükümler uygulanarak yasal süreç başlatılacaktır.

1. **SORUMLULAR:**

BGYS politikalarının, gözden geçirilmesi ve güncellenmesinden Bilgi Güvenliği Ekibi sorumludur. Rektör makamı tarafından Bilgi Güvenliği Politikası onaylanır ve duyurulması sağlanır. Bu politikalardan tüm çalışanlar, öğrenciler, tedarikçiler ve ziyaretçiler sorumludur.

1. **UYGULAMA:**

**5.1 POLİTİKA LİSTESİ**

* P01 İnternet Erişim Politikası
* P02 E-Posta Politikası
* P03 Anti-Virüs Politikası
* P04 Şifre Politikası
* P05 Fiziksel Güvenlik Politikası
* P06 Sunucu Güvenlik Politikası
* P07 Ağ Yönetimi Politikası
* P08 Uzak Bağlantı Politikası
* P09 3. Taraf Güvenlik Politikası
* P10 Kabul Edilebilir Kullanım Politikası
* P11 Temiz Masa Temiz Ekran Politikası
* P12 Mobil Cihaz Politikası
* P13 Veritabanı Güvenlik Politikası
* P14 Yazılım Temini Ve Geliştirme Politikası
* P15 Değişim Yönetimi Politikası
* P16 Olay Yönetim Politikası
* P17 Kriptografik Kontroller Politikası
* P18 Kamera Politikası
* P19 Yedekleme Politikası
* P20 Web Tahsisi Politikası

**5.2 BİLGİ GÜVENLİĞİ UYGULAMA POLİTİKALARI**

# **P01 İNTERNET ERİŞİM POLİTİKASI**

1. **Amaç**

Kurum içinde güvenli internet erişimi için sahip olması gereken standartların uygulanmasını amaçlamaktadır. İnternetin uygun olmayan kullanımı; kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bu tür olumsuzlukların gerçekleşmemesi için etik ve yasalar çerçevesinde internet kullanım kurallarını belirlemektir.

1. **Kapsam**

Bu politika kurum internetini kullanan çalışanları, öğrencileri, tedarikçileri ve ziyaretçileri kapsamaktadır.

1. **Politika**

* Kurum ağlarına bağlı tüm bilgisayarlar içerik denetimi yapan bir uygulama üzerinden internete çıkacaktır. Kurum kültürüne ve yasalara uygun olmayan siteler yasaklıdır. Ancak yetkilendirilmiş sistem yöneticileri ve kişiler internete çıkarken bütün servisleri kullanma hakkına sahiptir.
* 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) gereği kurum internet erişim kayıtları en az 24 ay arşivlenmektedir.
* Bilgisayarlar üzerinden yasalara aykırı internet sitelerine girmek ve dosya (film, dizi, müzik, program vb.) indirmek yasaktır.
* Tunnel platformları (VPN), proxy ve dns değişiklikleri yapılarak internete bağlanılması yasaktır.
* Başkalarının fikri haklarını ihlal edici mahiyette (copyright) materyalin (yazı, makale, kitap, film, müzik eserleri vb.) dağıtımı yasaktır.

Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Kurum bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa 2547 sayılı Yükseköğretim Kanunu ve 657 sayılı Devlet Memurları Kanunu’nun disiplin ve ceza işlerine ilişkin hükümleri, öğrenciler hakkında Yükseköğretim Kurumları Öğrenci Disiplin Yönetmeliği uygulanacak, disiplin işlemlerinin yanı sıra eylemin niteliğine uygun olarak ilgili mevzuat hükümleri uyarınca yasal işlem yapılacaktır. Tedarikçi ve ziyaretçiler için ise genel hükümler uygulanarak yasal süreç başlatabilir.

* İnternet üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ile kuruma ve kurumun çalışanlarına, bunların aile fertlerine veya Türkiye Cumhuriyeti devletine, ulusuna, yasama, yürütme ve yargı organlarına, askeri ve emniyet teşkilatına, vatandaşlarına yönelik iftira, karalama mahiyetinde mesajlar yayınlamak ve paylaşmak yasaktır.
* Kullanıcıların internet üzerinden görevleri ile ilgisi bulunmayan, internet trafiğini kısıtlayabilecek veya zarar verebilecek online olarak yayın yapan televizyon, radyo, film, canlı kamera yayınları, sosyal medya, oyun vb. içerikli yayınların kullanılması yasaktır.
* Kullanıcıların kurumsal e-posta adresleri ile forum, alışveriş vb. sitelere üye olması yasaktır.
* Kullanıcıların kurum hesaplarına ait kullanıcı adı ve şifreleri internet üzerinden paylaşması yasaktır.
* Kullanıcıların kurum internet ağı üzerinden yaptığı kişisel işlemlerde (banka, alışveriş, e-posta vb.) oluşacak olumsuzluklardan kurum sorumlu değildir, bu tür sebepler ile kurum veya kişisel hesabının bir başkasının eline geçmesine sebep olunması ve bu durumda gerçekleştirilebilecek muhtemel suçlardan kişi mesuldür.
* İnternette gezinirken reklam veya bilgi çalmak amaçlı (tebrikler, ödül kazandınız, ödülünüzü almak için tıklayın vb.) aldatıcı resim ve yazılara karşı dikkatli olunmalı ve tıklanmamalıdır.
* **P02 E-POSTA POLİTİKASI**

1. **Amaç**

Kurumsal e-postaların standartlara uygun, kesintisiz kullanım ve güvenliğinin sağlanması amaçlanmaktadır.

1. **Kapsam**

Bu politika kurum e-postasını kullanan çalışanları ve öğrencileri kapsamaktadır.

1. **Politika**

* Kullanıcıların kurum e-postalarından gönderdikleri, aldıkları veya sakladıkları e-postalar Karabük Üniversitesi’nin bilgi varlığıdır. Bu nedenle kurumsal e-postaları yetkili kişiler gerekli durumlarda önceden haber vermeksizin denetleyebilir ve yasa uygulayıcıları ile paylaşabilir.
* Kişisel amaçlar için kurumsal e-posta kullanımı yasaktır ve Karabük Üniversitesinin kullanıcılar ile e-posta yedeklerini paylaşma zorunluluğu yoktur.
* Karabük Üniversitesi ile ilgili Gizli/Kritik verileri içeren bilgiler e-posta, internet dosya paylaşım siteleri, paylaşım yazılımları ile gönderilemez.
* Açılan e-postaları geçici şifre ile açılmaktadır, 90 gün içerisinde değiştirilmesi gerekmektedir.
* Çalışanların kişisel kullanım için kurumsal e-posta adresleri ile forum, alışveriş vb. sitelere üye olması yasaktır.
* Karabük Üniversitesinin toplu e-posta gönderi gruplarına, kişisel kullanım amaçlı e-posta gönderilmesi yasaktır. Bilimsel, akademik ve idari iş süreçlerine uygun toplu duyurular ise Karabük Üniversitesi Basın Yayın ve Halkla İlişkiler Birimi tarafından (Rektörlük onayı doğrultusunda) yapılmaktadır.
* Kurumsal e-posta; yasadışı, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik spam, sahte, zincir e-posta ve bu e-postalara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postaların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir e-posta alındığında hemen Bilgi İşlem Daire Başkanlığına veya Bilgi Güvenliği Ekibine haber verilmesi ve yetkili kişiler müdahale edene kadar e-postanın silinmemesi, yanıtlanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.
* E-posta gönderen kullanıcılar; e-posta içeriğini dikkate alarak, sadece ilgili kişilere göndermelidir. E-posta gönderilmeden önce “Kime” ve “Bilgi” bölümlerine eklenen kişi listesi kontrol edilmelidir.
* Kullanıcılar, e-posta içeriğine kullanıcı adı ve şifre yazmamalıdır. Kullanıcı adı ve şifre talep edilen e-postalar alındığında hemen Bilgi İşlem Daire Başkanlığına veya Bilgi Güvenliği Ekibine haber verilmesi ve yetkili kişiler müdahale edene kadar e-postanın silinmemesi, yanıtlanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.
* Kullanıcıların; kurumsal e-posta ile uygun olmayan içeriklere sahip e-posta (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyeti ihlal eden ve hakaret içeren vb.) göndermeleri yasaktır.
* Karabük Üniversitesinin idari yapısı içinde yer alan birimlerde akademik/idari görevlerde bulunan personel ile @karabuk.edu.tr , Karabük Üniversitesinde öğrenim hayatını sürdürmekte olan tüm öğrencilere @ogrenci.karabuk.edu.tr uzantılı kurumsal e-posta hesabı tanımlanmaktadır. Ayrıca Kullanıcılar <http://bislem.karabuk.edu.tr/formlar> adresinde “Webmail Talep Formları” ile de e-posta talebinde bulunabilmektedir.
* Üniversitede hizmet alımı ile çalışan personele birinci veya ikinci derece sorumlu birim amiri onayı ve talebi doğrultusunda e-posta hesabı açılabilmektedir. Birim amiri tarafından çalışan personelin görevinin sonlandırıldığının Bilgi İşlem Daire Başkanlığına bildirilmesi zorunlu olup bildirim doğrultusunda e-posta hesabı kapatılmaktadır.
* Üniversitede tüm akademik/idari birimler adına birinci veya ikinci derece sorumlu birim amiri onayı ve talebi doğrultusunda birim e-posta hesabı açılabilmektedir.
* Kullanıcı; gizli e-posta içeriğini ilgisi bulunmayan kişilere göstermeyeceğini, hizmet hakkının sadece kendisine ait olduğunu, bu hakkın kullanımına ilişkin özel ve gizli şifresini ve kullanıcı adını ve/veya kodunu başkasına kullandırmayacağını ve devretmeyeceğini, başkası tarafından öğrenilme şüphesi dahi olsa derhal değiştireceğini, aksi takdirde yapılan tüm işlemlerin sorumluluğunun kendisine ait olacağını, kendisi kullanmadığı iddiası ile sorumluluktan kurtulamayacağını kabul eder.

Karabük Üniversitesi personelinin; kurum kimliği altında sürdürülen tüm faaliyetler için kuruma ait “@karabuk.edu.tr” uzantılı kurumsal e-posta adresine sahip olması, ilgili yazışmalar ve talepler için kurumsal e-posta hesabını kullanması gerekir.

* Kullanıcı; hesabında ticari reklamlara ve üyelik ile sağlanan yerli/yabancı destekleyici (sponsor) reklamlarına, bağlantılarına yer veremez. Ticari reklamlar ve haber duyuruları gibi istenmeyen mesajlar gönderemez.
* Kullanıcı şifresi sadece kullanıcı tarafından bilinir. Kullanıcı ilk kullanımdan itibaren dilediği zaman e-posta şifresini değiştirebilir. Şifrenin seçimi ve korunması tamamıyla kullanıcının sorumluluğundadır. Şifre değiştirme işlemi login.microsoftonline.com adresinde oturum açıldıktan sonra hesap/güvenlik sekmesinden yapılabilmektedir.
* Kullanıcı hesabı;
  + T.C. yasalarının belirlediği yasadışı kullanımlarda,
  + Karabük Üniversitesi tarafından belirlenen kullanım politikalarına uyulmadığı durumlarda,
  + Kullanıcı hesapları için belirlenen sınırların aşıldığı durumlarda,
  + Karabük Üniversitesi bilişim kaynaklarının akademik amaçlı çalışmaları engelleyici biçimde akademik amaçlı olmayan, ticari ve yasadışı amaçlı kullanıldığı durumlarda,
  + Kişilere ait kullanıcı hesaplarının farklı kişiler tarafından kullanımının belirlendiği durumlarda,
  + Sunucu sistemler üzerinde tanımlı diğer kullanıcıların şifrelerini bulmaya çalışmak, dosyalarına müdahale etmek, değiştirmek vb. girişimlerin tespit edildiği durumlarda,
  + Sistem doğruluğunun, bütünlüğünün, güvenliğinin ve servis devamlılığının engellendiği durumlarda,

Kullanıcıya haber verilmeksizin Bilgi İşlem Daire Başkanlığı tarafından geçici olarak kapatılabilir. Çalışanlara ait e-posta hesaplarının kalıcı olarak kapatılacağı durumlarda kullanıcılar önceden bilgilendirilir.

* **P03 ANTİ-VİRÜS POLİTİKASI**

1. **Amaç**

Bilgisayar ve sunucuların zararlı yazılımlardan korunması amaçlanmaktadır.

1. **Kapsam**

Bu politika tüm bilgisayarları ve sunucuları kapsamaktadır.

1. **Politika**

* Kurumun bütün bilgisayarları ve sunucuları Anti-virüs yazılımına sahip olacaktır.
* Hiç bir kullanıcı herhangi bir sebepten dolayı Anti-virüs programını sistemden kaldıramaz veya durduramaz.
* Anti-virüs yazılımı düzenli aralıklar ile otomatik veya manuel olarak güncellenecektir.
* Anti-virüs yazılımı haftalık olarak bilgisayar ve sunucularda virüs taraması yapacaktır.
* Virüs bulaşan makineler tam olarak temizleninceye kadar ağa bağlanmayacaktır. Bilgisayarlarda virüs olduğu uyarısı alındığında veya şüpheli durumlarda hemen Bilgi İşlem Daire Başkanlığı’na veya Bilgi Güvenliği Ekibine haber verilmesi ve yetkili kişiler müdahale edene kadar bilgisayarın kullanılmaması gerekmektedir.
* İnternet üzerinden bilinmeyen ve şüpheli kaynaklardan indirilen dosyaların içerisinde virüs olma ihtimali nedeniyle bu tür kaynaklardan dosya indirilmemelidir.
* Bilgisayarlarda kullanılacak CD, DVD, USB gibi depolama aygıtlarını ve internet üzerinden indirilen dosyalar virüs taraması yapmadan kullanılmamalıdır.
* Kurumun kullanıcı bilgisayarlarına antivirus programını kurmakla sorumlu olan kullanıcının kendisidir, kullanıcı antivirus programı kurmadığı taktirde sorumluluk kendisine aittir.
* Bilgi İşlem Daire Başkanlığı’nın hazırlamış olduğu bilgisayarlar güncellemeleri yapılmış anti virüs yazılımı yüklenmiş şekilde kurum ağına dâhil edilir. Bilgi İşlem Daire Başkanlığı kontrolü dışında alım yapılan bilgisayarlara <https://www.bislem.karabuk.edu.tr> adresinde bulunan Kullanıcı Girişini kullanarak dosya deposundaki lisanslı anti virüs programı indirilerek kurulması ve güncel tutulması zorunludur.

**P04 ŞİFRE POLİTİKASI**

1. **Amaç**

Bilgi Güvenliğinin arttırılması için güçlü bir şifreleme oluşturulması ve şifrelerin güvenliğinin sağlanması amaçlanmaktadır.

1. **Kapsam**

Bilgisayar, sunucu, uygulama, tüm network cihazları ve epostaları kullanan tüm kullanıcı hesaplarını kapsamaktadır.

1. **Politika**

* Bilgisayar kullanıcı hesaplarının şifreleri en az 8 karakter ve karmaşık şekilde büyük harf, küçük harf, rakam ve özel karakter (\ \* ? - = / \_ + % & vb.) kullanılması zorunludur. Türkçe karakter kullanmamaya özen gösterilmelidir.
* Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kolay tahmin edilen (Aa123456, Ab123456, Qaz12345, Asd12345, memleket, çocuk, çalışanın kendi ismi, doğum tarihi, ardışık rakam ve harfler, İstanbul, Karabük vb.) şifreler kullanılmamalıdır.
* Kurum içerisinde kullanılan bilgisayar, uygulama ve eposta hesap şifrelerinin 90 günde bir değiştirilmesi gerekmektedir.
* Bilgi İşlem Daire Başkanlığı tarafından oluşturulan yeni şifreler ilk kullanımdan itibaren değiştirilmelidir.
* Kurumsal hesaplara ait şifrelerin herhangi bir kimseyle (iş arkadaşları, aile bireyleri vb.) paylaşılmamalıdır.
* Kurumsal hesaplara ait şifrelerin kağıt veya elektronik ortamlara (e-posta, word, excel, forum siteleri vb.) yazılmamalı ve paylaşılmamalıdır.
* Kurum içinde kullanılan diğer uygulamaların (Yönetim programları, Firewall, Mail Sunucusu, Ortam Denetleme vb.) şifreleri de Şifre Politikasına uygun olarak tanımlanacaktır.

**P05 FİZİKSEL GÜVENLİK POLİTİKASI**

1. **Amaç**

Kurumun bilgi varlıkları, ekipmanları ve alt yapı cihazlarının fiziksel güvenliği ve yetkisiz erişimlerinin önlenmesi amaçlanmaktadır.

1. **Kapsam**

Kurumun bilgi varlıkları, ekipmanları ve alt yapı cihazlarını kullananları kapsamaktadır.

1. **Politika**

* Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanacak ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilecektir.
* Bilgi İşlem Daire Başkanlığına girişler, dış cephe ve koridorlar güvenlik açısından kamera ile kayıt altına alınarak izlenmektedir. Kamera kayıtları en az 90 gün saklanmaktadır.
* Açık ofislerde ve odalarda bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulacaktır.
* Kurumun bilgi varlıkları, bilgisayar ve çevre birimleri (harici diskler, yazıcı, monitör, projeksiyon vb.), alt yapı cihazlarını hasar / hırsızlık gibi oluşabilecek risklere karşı önlem almak ve güvenliği açısından uyarı yazıları yazmak kişi ve birimin kendi sorumluluğundadır.
* Kritik bilgi varlıkları ve altyapı cihazları kilitli odalarda ve kabinetlerde muhafaza edilecektir.
* Erişim yetkisi verilerek girilen alanların erişim yetkileri düzenli aralıklar ile kontrol edilecektir.

**P06 SUNUCU GÜVENLİK POLİTİKASI**

1. **Amaç**

Bilgi İşlem Daire Başkanlığının sahip olduğu sunucuların temel güvenlik kurallarını oluşturmayı amaçlamaktadır.

1. **Kapsam**

Bu politika Bilgi İşlem Daire Başkanlığının sahip olduğu bütün sunucuları kapsamaktadır.

1. **Politika**

* Kurum bünyesindeki bütün sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.
* Tüm sunuculara Bilgi İşlem Daire Başkanlığı’nın yetkilendirdiği kişiler dışında erişim yapılmamalıdır.
* Kullanılmayan sunucular güvenlik, performans ve elektrik tasarrufu açısından kapalı tutulmalıdır.
* Sunucuların kaynakları (cpu, ram, disk, ağ trafiği vb.) düzenli olarak izlenecektir.
* Sunuculara dışarıdan yapılan bağlantılar Uzak Bağlantı Politikasının belirlediği kurallara göre gerçekleştirilecektir.
* Sunucular fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulundurulacaktır.
* Sistem odaları sıcaklık, nem değerleri ve su basmasına karşı denetlenecektir.
* Sistem odası sıcaklık derecesi tavsiye edilen (20-24) seviyede tutulacak şekilde soğutulacaktır.
* Sistem odalarına giriş ve çıkışlar erişim kontrollü olacak ve kayıt altına alınacaktır.
* Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunacaktır, yangın ve benzer felaketlere karşı koruma altına alınacaktır.
* Sunucularda anti-virüs programı yüklü olacak ve anlık olarak tarama yapacaktır.

**P07 AĞ YÖNETİMİ POLİTİKASI**

1. **Amaç**

Kurumun bilgi teknolojileri ağında yer alan bilgilerin, ağ alt yapısının ve ekipmanlarının güvenliğini ve sürekliliğini sağlamayı amaçlamaktadır.

1. **Kapsam**

Kurum bünyesindeki ağ altyapısı, donanım ve kullanıcıları kapsamaktadır.

1. **Politika**

* Üniversitenin ağ alt yapısındaki, donanımı ve yazılımı zarara uğratan, tahrip edici, zedeleyici ve sağlıklı çalışmasını engelleyici hiçbir girişimde bulunulmaması; kaynakların verimli kullanılması en temel ilkedir.
* Üniversitenin ağ hizmetleri Türkiye Cumhuriyeti yasalarına ve Üniversite yönetmelikleri başta olmak üzere yasalara bağlı olan yönetmeliklere aykırı faaliyetlerde bulunmak amacıyla kullanılamaz.
* Üniversitenin ağ hizmetleri akademik ve idari işlemlerin görülmesi amacıyla verilmektedir. Diğer kullanımlar, ancak bu kullanım gereksinimleri karşılandıktan sonra arta kalan zaman ve kapasite boyutlarında gerçekleştirilebilir.
* Üniversitenin ağ alt yapısı ve bilgisayar ağı üzerinde yer aldığı Ulusal Akademik Ağ (ULAKNET) ve diğer ulusal ve uluslararası ağların kullanım politikalarına, bilişim kaynaklarını kullanan tüm birimlerin ve tüm kullanıcıların uyma ve bu bağlamda gerekli önlemleri alma zorunluluğu vardır.
* Ağ ekipmanları Bilgi İşlem Daire Başkanlığının yetkilendirdiği kişiler tarafından erişilebilecek ve yönetilebilecektir. Kurum ağına ve ağ ekipmanlarına yetkisiz erişim olmamalıdır.
* Kurum ağı, sadece kurum bilgisayarları, ağ ekipmanları ve mobil cihazlar bağlanacak şekilde yönetilmektedir.
* Misafirlere kablosuz internet bağlantısı kayıt işlemleri yapıldıktan sonra verilmektedir.
* Bilgi teknolojileri ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için yedek ağ ekipmanları bulundurulacaktır.
* Uzaktan bağlantı için kullanılacak portların güvenliği sağlanacaktır.
* Ağ cihazları yılda en az 1 defa açıklık (sızma) tarama testlerinden geçirilerek zafiyetler tespit edilecek ve gerekli tedbirler alınarak güvenli hale getirilecektir.
* Kurumun bilgi teknolojileri ağı detaylı olarak takip (monitoring) ve analiz edilecektir.
* Kabin yerleri, birimlerdeki ağ alt yapısı kurulurken, internet erişiminin en verimli şekilde kullanılması, ağ alt yapısı masraflarını ve kablo mesafelerine bağlı olarak veri kayıplarının en aza indirgenmesi dikkate alınarak belirlenir. Üniversite internet kullanıcıları kabin ve kabin odalarıyla ilgili aşağıdaki kurallara uymak zorundadır.

1. Bilgi İşlem Daire Başkanlığı çalışanlarının haricinde hiçbir kullanıcı kabin içerisine müdahalede bulunamaz.
2. Kabinleri besleyen elektrik prizlerine, sigortalara ve kesintisiz güç kaynağına müdahalede bulunamaz.
3. Kabinlerin üzerine eşya, yakınına sıvı maddeler konulması ve kabinin güvenliğini bozacak her türlü durum için ortaya çıkabilecek sorunlardan ilgili tüm birimler sorumludur.

* Üniversitenin ağ hizmetleri kaynaklarının herhangi bir amaçla kullanım hakkı, Bilgi İşlem Daire Başkanlığı ve Rektörlükçe onay verilmeden üçüncü özel veya tüzel kişilere verilemez.
* Bilgi İşlem Daire Başkanlığının bilgisi dışında ağ kurmak, aktif-pasif cihazları ağa eklemek veya kablosuz yayın yapmak kesinlikle yasaktır.
* Üniversitede kablosuz ağ kullanıcıları, ağ üzerinde kendilerine verilen kullanıcı yetkisini ve kullanıcı kodunu, şifresini kullanarak bu kaynaklar üzerinde gerçekleştirdikleri çalışmalar ve etkinlikler ile bu kaynaklar üzerinde bulundurdukları veya oluşturdukları bilgi, belge, yazılım gibi her türlü kaynağın içeriğinden ve kullandıkları kaynakların kullanım kurallarına uyulmasından şahsen sorumludur.
* Bilgi İşlem Daire Başkanlığının sağladığı güvenlik çözümleri haricinde kullanılan kişisel güvenlik çözümlerinin kullanılmasıyla birlikte oluşacak sorunlardan kişi kendisi sorumludur.
  + Veri kablosu, sonlandırma ve aktarma işlemlerinde kullanılan bütün bileşenlerin (patch panel, veri prizi, patch kablolar vs.) uluslararası kablolama standartlarına uygun olarak kullanılması zorunludur.
  + Kampüsler içinde ve binalar arasında dolaşan fiber optik (F/O) hattının zarar görmemesi için gerekli önlemleri almak ve bu fiber ağının geçtiği yerlerde yapılan inşaat, kazı ve diğer faaliyetleri denetlemek ve oluşabilecek sorunların tamir onarımını yapmak Bilgi İşlem Daire Başkanlığının sorumluluğunda değildir.
  + Cihazların ve bu cihaza bağlı ekipmanların fiziki sorumlulukları, cihazın bulunduğu yerin (bina, kat laboratuvar vs.) birim amiri ve birim amirinin belirlemiş olduğu oda ve kabin sorumlusuna aittir.

**P08 UZAK BAĞLANTI POLİTİKASI**

1. **Amaç**

Kurumun bilgi teknolojileri sistemlerine dışarıdan yapılacak olan uzak bağlantıların güvenliğinin sağlanması amaçlanmaktadır.

1. **Kapsam**

Bu politika bilgi teknolojileri sistemlerine dışarıdan bağlantı yapacak tüm kurum çalışanlarını ve paydaşlarını kapsamaktadır.

1. **Politika**

* Uzaktan bağlantı kurum personeli için sadece SSL VPN ile yapılmaktadır. Tedarikçi firmaların erişimleri için IP adresi özel izin verilmektedir.
* Kurum paydaşları uzak bağlantı için e-posta yoluyla talepte bulunacaktır ve onay dahilinde erişim sağlanacaktır.
* VPN kullanım hakkı verilen kişiler listelenecek ve düzenli olarak kontrol edilecektir.
* VPN kullanım hakkı verilen kişilerin kullanıcı hesap bilgilerini başkalarıyla paylaşması yasaktır.
* Kurum bilgisayarları haricinde VPN bağlantısı yapılacak cihazlarda anti-virüs yazılımları kurulu ve güncel olmak zorundadır.
* Kurum gerekli gördüğü durumlarda herhangi bir uyarıda bulunmadan VPN bağlantı erişimlerini kesme hakkına sahiptir.

# **P09 3. TARAF GÜVENLİK POLİTİKASI**

1. **Amaç**

Kurumun bilgi teknolojilerine ve bilgi varlıklarına üçüncü taraflar tarafından ulaşılması durumunda güvenliğinin sağlanması amaçlanmaktadır.

1. **Kapsam**

Bu politika Bilgi İşlem Daire Başkanlığı çalışanları ve paydaşları (tedarikçiler, müşteriler, ziyaretçiler, bakım firmaları vb.) kapsamaktadır.

1. **Politika**

* Kurum paydaşları ile bilgi teknolojileri sistemlerimize veya bilgi varlıklarına müdahale, test, bakım onarım vb. amaç ile geldiklerinde Gizlilik Sözleşmesi yapılacaktır ve bulundukları sürece kurum politikalarına uygun hareket etmekle yükümlüdürler.
* Kurum paydaşları ile Bilgi İşlem Daire Başkanlığına ait özel bilgilerin paylaşıldığı proje veya iş anlaşmaları durumunda Gizlilik Sözleşmesi yapılacaktır.
* Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarımız üzerinde yapacakları çalışmaları Karabük Üniversitesi Bilgi İşlem Daire Başkanlığına bildirmek zorundadır.
* Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarına, kendilerine verilen yetki kapsamında erişim sağlayacaktır.
* Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarına erişim yetkileri, çalışma alanlarını kapsayacak şekilde kısıtlı yetki verilecektir. İşlem logları saklı tutulacak ve çalışma bittikten sonra verilen yetkiler hemen geri alınacaktır.
* Kurum paydaşlarına bilgi teknolojileri sistemlerimize veya bilgi varlıklarına erişim izni verilecek bilgisayarlar/mobil cihazlar için UZAK BAĞLANTI POLİTİKASI uygulanacaktır. Kurum gerekli gördüğü durumlarda herhangi bir uyarıda bulunmadan VPN bağlantı erişimlerini kesme hakkına sahiptir.

**P10 KABUL EDİLEBİLİR KULLANIM POLİTİKASI**

1. **Amaç**

Bilgi teknolojileri sistemlerine ve bilgi varlıklarına Gizlilik, Bütünlük ve Erişilebilirlik sınıfları açısından yapılması ve uyulması gereken iş kurallarını çalışanlara bildirmeyi amaçlamaktadır.

1. **Kapsam**

Bu politika tüm Üniversite birimleri/çalışanları ve paydaşları (tedarikçiler, vatandaşlar, ziyaretçiler vb.) kapsamaktadır.

1. **Politika**

* Çalışanlar, kurumun kendilerine tahsis etmiş olduğu bilgisayarlar veya cihazlar üzerinde kişisel veri bulunduramaz. Bu cihazlar kuruma aittir ve iş amaçlı kullanım için verilmiştir. Kurum gerekli gördüğünde çalışana herhangi bir uyarıda bulunmadan bu cihazları geri alma hakkına sahiptir.
* Kurum bilgisayarının veya cihazlarının, çalışandan alınması durumunda; çalışanın cihazlar üzerindeki kişisel verileri için erişim yetkisi istemesi halinde Üst Yönetim bilgisayar veya cihazlara erişim izni vermeme hakkına sahiptir.
* Kuruma ait gizli tüm bilgilerin gizliliğine uyulması zorunludur. Bu bilgilerin izinsiz olarak kopyalanması, çoğaltılması, paylaşılması ve iletilmesi yasaktır.
* Tüm çalışanlar, kendilerine tahsis edilmiş bilgisayar / cihazların erişim bilgilerini ve güvenliğini korumakla sorumludur ve paylaşması yasaktır.
* Çalışanların, bilgisayarından anti-virüs koruma yazılımını devre dışı bırakması yasaktır.
* Çalışanların kuruma ait bilgisayar ve cihazlarda kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir yazılımı kullanması veya kopyalaması yasaktır.
* Kuruma ait bilgisayarlara ve cihazlara lisanssız program yüklenmesi yasaktır.
* Kullanıcıların kurumun kendilerine tahsis etmiş olduğu bilgisayar, cihaz ve kurum dosya sunucusu üzerinde kuruma ait bilgi, belge ve programlar haricinde (müzik, film vb.) dosya bulundurması veya paylaşması yasaktır.
* Kritik dokümanlara erişim yetkisi bulunan kullanıcı, doküman içeriğindeki bilginin uygun bir şekilde korunmasından sorumludur.
* Herhangi bir kişi kendine ait olmayan kritik veri bulur ise bu durumu Bilgi İşlem Daire Başkanlığına bildirmekle yükümlüdür.
* Çalışanlar, “Gizli” belgeleri kilitli dolaplarda muhafaza edecektir.
* Sunucu ve bilgisayarların saatleri kullanıcılar tarafından değiştirilmemelidir.
* Çalışan, taşınabilir cihazları (laptop, tablet, cep telefonu, harici disk vb) güvenlik açıklarına karşı daha dikkatle korumak zorundadır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır.
* Çalışanların kurumun tahsis ettiği bilgisayar ve cihazları kendisi dışında herhangi bir kimseye (iş arkadaşları, aile bireyleri vb.) kullandırması ve paylaşması yasaktır.
* Kullanıcıların program yükleme ve PC’lerindeki diğer iş talepleri EBYS üzerinden gerçekleştirilecek ve Bilgi İşlem Daire Başkanlığı tarafından yönetilecektir.

**P11 TEMİZ MASA TEMİZ EKRAN POLİTİKASI**

1. **Amaç**

Çalışanların mesai saatleri içi veya dışında görevleri gereği kullandığı bilgilerin (yazılı doküman, belgeler, formlar, bilgisayarlar vb.) yetkisiz erişim veya uygunsuz kullanımı sonucunda oluşabilecek riskleri ortadan kaldırmayı amaçlamaktadır.

1. **Kapsam**

Bu politika kurumun tüm çalışanlarını kapsamaktadır.

1. **Politika**

* Çalışma masasından ayrıldığında basılı doküman ya da taşınabilir depolama aygıtları üzerinde tutulan bilgiler güvenlikli ortamlarda (çelik kasa, kilitli dolap ve çekmeceler vb.) saklanacaktır.
* Her türlü faks, fotokopi, yazıcı vb. cihazlar üzerinde yetkisiz erişimlere karşı belge, doküman vb. bırakılmayacak ve sürekli kontrol edilecektir.
* Bilginin kullanıldığı sistemler (sunucular, kamera DVR cihazları, bilgisayar, cep telefonları vb.) şifresiz kullanılmayacak ve korumasız bir şekilde bırakılmayacaktır.
* Bilgi teknolojileri sistemlerinde kullanılan kullanıcı adı ve şifreler bilgisayar veya masa üzerinde yazılı olarak bulundurulmayacaktır.
* İhtiyaç duyulmadığına karar verilen dokümanlar ve içinde bilgi bulundurulabilecek elektronik cihazlar uygun metotlarla (kâğıt öğütücü, disk/disket kıyıcı, yakma vb.) imha edilecektir.
* Gizli olarak tanımlanan (sözleşme, fatura, kişisel veri içeren, şartnameler, veri dokümanları vb.) dokümanlar ve kopyaları, müsvedde olarak kullanılmayacak ve kâğıt öğütücü ile imha edilecektir.
* Kullanıcılar bilgisayarlarının masaüstlerindeki dosyalarını, düzenli olması için klasörler içerisinde muhafaza edeceklerdir.

**P12 MOBİL CİHAZ POLİTİKASI**

1. **Amaç**

Kuruma ait bilgi içeren mobil cihazların güvenli kullanım ve yönetimini amaçlamaktadır.

1. **Kapsam**

Kuruma ait bilgi içeren tüm mobil ve taşınabilir cihazları kapsar.

1. **Politika**

* Kuruma ait mobil cihazlar (cep telefonu, dizüstü bilgisayar, usb bellek, harddisk, tablet vb.) ilgili kişiye zimmetlenerek teslim edilmelidir.
* Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.
* Kuruma ait bilgi içeren mobil cihazlara yetkisiz müdahaleyi önlemek için kullanıcı tarafından şifre tanımlanması zorunludur.
* Kurum telefon hatları ve mobil cihazlar üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ve başkalarına iftira, karalama mahiyetinde iletişim kurmak, mesajlar yayınlamak ve paylaşmak yasaktır.
* Kurumun tahsis ettiği mobil cihazların kendisi dışında herhangi bir kimseye (iş arkadaşları, aile bireyleri vb.) kullandırılması ve paylaşılması yasaktır.
* Mobil cihazlarda ne tür bilgiler saklandığının farkında olunmalı ve kuruma ait bilgiler mümkün olduğunca mobil cihazlar üzerinde bulundurulmamalıdır.

**P13 VERİTABANI GÜVENLİK POLİTİKASI**

1. **Amaç**

Kurumun veri tabanı sistemlerinin güvenli kullanım ve yönetimini amaçlamaktadır.

1. **Kapsam**

Bilgi İşlem Daire Başkanlığının sorumluluğundaki tüm veri tabanı sistemlerini kapsar.

1. **Politika**

* Veri tabanında kritik verilere her türlü erişim işlemlerinin (okuma, değiştirme, silme, ekleme) log kayıtları tutulacaktır. Log kayıtlarına, Bilgi İşlem Daire Başkanlığı’nın yetkilendirdiği kişiler dışında erişim yapılması yasaktır.
* Veri tabanı bulunan sunuculara, Bilgi İşlem Daire Başkanlığı’nın yetkilendirdiği kişiler dışında erişim yapılması yasaktır.
* Sunucularda bulunan veri tabanlarının kritiklik seviyelerine göre yedekleri alınacaktır.
* Veri tabanı sunucuları fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulundurulacaktır.
* Veri tabanı bulunan medyalar (harici disk, usb bellek vb.) kurum dışına çıkarılmayacaktır.
* Veri tabanlarına kurum dışından erişimler Uzak Bağlantı Politikası’na uygun şekilde yapılacaktır.
* Veri tabanı sunucularının kaynakları (cpu, ram, disk, ağ trafiği vb.) düzenli olarak kontrol edilecektir.
* Veri tabanlarına kurum dışından erişim sağlayan firmalar ile Bilgi İşlem Daire Başkanlığı Gizlilik Sözleşmesi imzalanacaktır.

# **P14 YAZILIM TEMİNİ ve GELİŞTİRME POLİTİKASI**

1. **Amaç**

Kurumun yazılım temini ve geliştirme ihtiyacının güvenli yönetilmesini amaçlamaktadır.

1. **Kapsam**

Tüm yazılım temini ve geliştirmelerini kapsar.

1. **Politika**

* Bilgi İşlem Daire Başkanlığı, kaynak yönetimini sağlamak, mevcut altyapıya ve kullanım amacına uygun yazılım projeleri gerçekleştirmek veya satın almakla yükümlüdür.
* Yazılım geliştirmede, ihtiyaç analizi, tasarım, geliştirme, deneme ve onaylama safhalarını içeren iş planı kullanılacaktır.
* Bilgi İşlem Daire Başkanlığı tarafından onayı alınmamış yazılımların (geliştirilen veya satın alınan) kurum içerisinde kullanılması yasaktır.
* Kuruma ait yazılımlar Varlık Envanteri Listesine eklenecek ve takip edilecektir.
* Web sayfalarının mevcut modülerinin log alınıp alınmadığı düzenli aralıklarla kontrol edilecektir.

**P15 DEĞİŞİM YÖNETİMİ POLİTİKASI**

1. **Amaç**

Kurumun bilgi teknolojileri sisteminde yapılması gereken yazılımsal ve donanımsal değişikliklerde süreklilik ve güvenliği sağlamayı amaçlamaktadır.

1. **Kapsam**

Bu politika kurumun tüm çalışanlarını kapsamaktadır.

1. **Politika**

* Yazılımsal ve donanımsal değişiklik talepleri Bilgi İşlem Daire Başkanlığı tarafından değerlendirilerek üst yönetime sunulur, yönetimin kararı doğrultusunda ilgili aksiyonlar alınır.
* Yazılımsal ve donanımsal değişiklikler yapılmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenerek ilgili kişilere bilgi verilecektir.
* Yazılımsal ve donanımsal değişiklikler gerçekleştirilmeden önce değişikliğin yapılacağı sistemlerin yedekleri alınacaktır.
* Sistemlerde yapılacak değişikliklerde ilgili üretici tarafından onaylanmış güncellemeler kullanılacaktır.
* Yazılımsal ve donanımsal değişiklikler sisteme alınmadan önce Bilgi İşlem Daire Başkanlığı veya ilgili alt birim tarafından onaylanacaktır.

**P16 OLAY YÖNETİM POLİTİKASI**

1. **Amaç**

Bilgi güvenliği olaylarının kayıt altına alınması ve yönetilmesini amaçlamaktadır.

1. **Sorumlular**

Bu politikanın uygulanmasından tüm personel sorumludur.

1. **Politika**

* Bilginin gizlilik, bütünlük ve erişilebilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumları düzenli olarak kayıt altına alınacaktır. Yaşanan olaylar Bilgi Güvenliği Olay Yönetimi Politikasına göre yönetilecektir.
* Yaşanan Bilgi Güvenliği olayları Bilgi İşlem Daire Başkanlığı Siber Olaylara Müdahale Ekibi ’ne (SOME) ([some@karabuk.edu.tr](mailto:some@karabuk.edu.tr)) e-posta veya telefon ( 0370 418 79 80 ) ile bildirilecektir.
* Kurum verilerine yönelik Bilgi Güvenliği ihlal olaylarının kaynağı SOME tarafından araştırılacak ve olayın önemlilik seviyesine göre müdahale edilecektir.
* Bilgi güvenliği olayı kanıtları olay sonlanana kadar (log, fotoğraf, video vb) SOME tarafından saklanacaktır.
* Yaşanan Bilgi Güvenliği olayları cezai ve hukuki mesuliyetle sonuçlanabilir. Kurum bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa disiplin yönetmeliğini uygulayabilir veya yasa uygulayıcısı ile işbirliği yapabilir.
* Bilgi Güvenliği olayları analiz edilerek tekrarlanmaması için gerekli önlemler alınacaktır.

**P17 KRİPTOGRAFİK KONTROLLER POLİTİKASI**

1. **Amaç**

Bilgi varlıklarının saklandığı sistemlerin ve bilgi varlıklarının transferinin gizliliğini veya bütünlüğünün şifreleme yöntemleri ile korunması amaçlanmaktadır.

1. **Kapsam**

Bu politikanın uygulanmasından tüm personel sorumludur.

1. **Politika**

* Gizli olarak ifade edilen bilgi varlıklarının paylaşımında güçlü şifreleme algoritması kullanılacaktır. Bu bilgi varlıklarının paylaşımı sırasında sıkıştırma programı (winrar, winzip v.b.) ile sıkıştırılarak şifrelenecektir.
* Mobil cihazlardaki verilerin korunmasında şifre kullanılmalıdır.
* Kurumsal e-posta hesabı kurulu akıllı telefonlarda telefon kilidi kullanılması zorunludur.
* Tanımlanan şifreler belirli aralıklarla değiştirilmelidir.
* Tanımlanan şifreler kolay tahmin edilmeyen karmaşık şifreler olmalıdır.
* Kurumun e-posta sistemi SSL sertifikası ile şifrelenmektedir.

**P18 KAMERA POLİTİKASI**

1. **Amaç**

Bilgi İşlem Daire Başkanlığındaki IP kameralar ile oluşturulan verilerin, belirli bir süre saklanması ve muhafazası konusunda gerekli önlemleri almaktır.

1. **Kapsam**

Bu politika Bilgi İşlem Daire Başkanlığının tüm çalışanlarını kapsamaktadır.

1. **Politika**

* Bilgi İşlem bünyesinde IP kameraların kayıtlarını tutmak için Server Storage kullanılmaktadır.
* Tüm IP kameraların kayıtları son 90 günü sunucularda tutulmaktadır.
* Bilgi İşlem Daire Başkanlığı bünyesindeki IP kameraların bakımlarını, onarımlarını kendi personeli ya da anlaştığı herhangi bir şirket personeli vasıtasıyla yapacak veya yaptıracaktır.
* Görüntü kayıtlarını Üniversite yönetiminin izni ve talebi ile resmi belge karşılığında verilir. Kayıtların depolanacağı alanı talepte bulunan kişi veya kurum sağlar.
* Bilgi İşlem Daire Başkanlığı güvenlik kamerası izleme noktalarının amacı dışında kullanıldığını ve Anayasanın 20. maddesindeki “özel hayatın gizliliği” ve “kişisel verilerin korunması” hükmünün gözetilmediğini tespit ettiğinde, birim yetkililerine ve Üniversite yönetimine bilgi vererek gerekli tedbirleri alır.

**P19 YEDEKLEME POLİTİKASI**

1. **Amaç**

Üniversite ağı ve cihazları üzerinde oluşturulan, kullanılan ve devamlılığı gerekli görülen verilerin saklanması ve muhafazası konusunda gerekli önlemleri almaktır.

Bu politikanın uygulanmasından tüm personel sorumludur.

1. **Kapsam**

Bilgi İşlem Daire Başkanlığının kontrolünde olan ve Üniversite bünyesinde oluşturulan verilerin (storage ve sunucularda) güvenli olarak yedeklenmesi, gerektiğinde kullanıma açılması ve ihtiyaç sonunda silinmesi için gerekli yöntemlerin belirlenmesini tanımlar.

Bilgi İşlem Daire Başkanlığı bünyesinde yedekleme Bilgi İşlem Daire Başkanlığının kurmuş olduğu sistem ve sanal sunucuların veri yedeklerini kapsar.

1. **Politika**
   * Bilgi İşlem Daire Başkanlığı kendi kontrolünde olan ve gerekli gördüğü tüm cihazların, sistemlerin, ağların vs. kayıtlarını kendi belirlediği süre içerisinde düzenli olarak almaktadır. Belirlenen zaman boyunca saklamakta ve belirlenen zaman dolduğunda da silmektedir.
   * Bilgi İşlem Daire Başkanlığı kontrolünde olmayan kullanıcıların kullandığı cihazlara ve sistemlere vs. ait olan kişisel ve özel verilerin yedeklenme ve saklanma işlemlerinden kullanıcı kendisi sorumludur. Bilgi İşlem Daire Başkanlığı herhangi bir veri kaybından ya da kaybolan verilerin kurtarılmasından sorumlu tutulamaz.
   * Bilgi İşlem Daire Başkanlığı bünyesinde kullanılan sunucu ve sistemlerin düzenli aralıklarla önem sırasına göre, teknik imkanlar dahilinde yedekleri alınmaktadır.

**P20 WEB TAHSİSİ POLİTİKASI**

1. **Amaç**

Karabük Üniversitesinin, kurumsal kullanıcılarına sağladığı alan adlarının kullanım yönergesini oluşturmak ve kullanım ilkelerini belirlemek.

1. **Kapsam**

Bu politika kuruma ait web sayfası kullanan tüm birimlerini/çalışanlarını kapsamaktadır.

1. **Politika**
   * Karabük Üniversitesi, alan adı (domain) ve alt alan adı (subdomain) hizmetini yalnızca kurum bünyesindeki fakülteler, enstitüler, yüksekokullar, meslek yüksekokulları, birimler, bölümler, müdürlükler, koordinatörlükler, öğrenci toplulukları, akademik ve idari personeller, konferanslar, toplantılar, sempozyumlar, kongreler, çalıştaylar, paneller vs. gibi kurumsal yapılara sağlamaktadır.
   * Üniversite bünyesindeki fakülteler, enstitüler, yüksekokullar, meslek yüksekokulları, birimler, bölümler, müdürlükler, koordinatörlükler, öğrenci toplulukları, akademik ve idari personeller, konferanslar, toplantılar, sempozyumlar, kongre, çalıştay, panel vs. gibi yapılar üniversitenin kurumsal kimliğinin bozulmaması için Bilgi İşlem Daire Başkanlığı tarafından sağlanan web sitelerini kullanacaklardır.
   * Alt Alan adı (subdomain) açma talepleri, Bilgi İşlem Daire Başkanlığına kurumsal e-posta yoluyla, EBYS üzerinden yazılı olarak veya form doldurularak yapılır.
   * Site içeriği ile ilgili olarak olası hukuki süreçlerden adına web alanı tahsis edilen birim tarafından yetki verilen sayfa yöneticisi sorumludur.
   * Üniversite ve öğrenci toplulukları tarafından organize edilen veya katılımda bulunulan ulusal/uluslararası etkinlik ve organizasyonlar için verilen alan adresleri ilgili birim yöneticisi ya da topluluk danışmanlarından yazılı talep gelmesi üzerine açılmaktadır.
   * Kullanıcı, web alanı hizmetinden faydalanırken Bilgi İşlem Daire Başkanlığı tarafından yayınlanan her türlü ihtar ya da bildirime uymayı beyan, kabul ve taahhüt eder. Kullanıcı, almış olduğu web alanı hizmetini üçüncü kişilere her ne ad altında olursa olsun kullandıramaz.
   * Kullanıcı kişisel web alanında barındırdığı tüm dosya, doküman ve programlardan, web sitesi ve e-posta hizmetleri ile kullanacağı ve faydalanacağı tüm işlemlerden kendisinin sorumlu olduğunu; söz konusu veri, bilgi, beyanların yasalara aykırılığından ve web alanında barındırdığı web sayfası ya da programların güvenlik açıkları nedeniyle başka bir sunucuya yapılacak saldırıdan doğabilecek tüm hukuki ve cezai sorumluluğu kendisi karşılamayı kabul ve taahhüt eder. Bu konuda doğabilecek sorunlardan Bilgi İşlem Daire Başkanlığına herhangi bir sorumluluk yüklenemez.
   * Bilgi İşlem Daire Başkanlığı kullanıcıların hizmet aldığı merkezi sunucular üzerinde herhangi bir zamanda teknik değişiklikler yapma hakkına sahiptir. Bu değişiklikleri önceden kullanıcılara bildirebileceği gibi, anlık olarak yapılabilecek değişikliklerin önceden duyurulamaması da mümkün olabilir. Kullanıcılar oluşacak veri kaybı vs. gibi konularda herhangi bir hak talep edemez.
   * Bilgi İşlem Daire Başkanlığı, birimlerin kendi imkânları ile hazırlamış oldukları web sitelerinde güvenlik açığı bulunmasından dolayı hizmet alan diğer kullanıcılarına veya üçüncü şahıslara herhangi bir şekilde zararlı olduğuna karar verdiği durumlarda hizmeti kesebilir veya müdahale edebilir.
   * Bilgi İşlem Daire Başkanlığı hukuka aykırı fiil ve eylemler tespit edildiği andan itibaren kullanıcıya haber vermeden kullanıcı hesaplarını geçici veya sürekli olarak kapatma veya silme hakkına sahiptir.
   * Bilgi İşlem Daire Başkanlığı, sağladığı hizmet içerisinde bulunan kullanıcı verilerinin hatalı kullanımlarından, veri içeriklerinden, e-posta ile kullanılan tüm verilerden doğabilecek hiç bir maddi veya manevi zararlardan sorumlu tutulamaz. Bu verilerin yedekleme ve saklama yükümlükleri kullanıcıya aittir.
   * Bilgi İşlem Daire Başkanlığı yedekleme işlemlerini bilişim politikalarında belirttiği yedekleme politikasına uygun olarak yapmaktadır.
   * Bilgi İşlem Daire Başkanlığı web programlama konusunda sadece gelen taleplere göre Üniversite bünyesindeki fakülteler, enstitüler, yüksekokullar, meslek yüksekokulları, birimler, bölümler, müdürlükler, koordinatörlükler, öğrenci toplulukları, konferanslar, toplantılar, sempozyumlar, kongreler vs. gibi kurumsal yapılara ve gruplara gerekli gördüğü takdirde web yazılım desteği sağlamaktadır.