GAZİ ÜNİVERSİTESİ

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

VARLIKLARIN KABUL EDİLEBİLİR KULLANIM POLİTİKASI

Revizyon Tarihçesi

Revizyon No	Revizyon Gerekçesi	Revizyon Tarihi

İçindekiler Tablosu

1. AMAÇ

Bu politikanın amacı, kurum personelinin ve üçüncü taraf çalışanlarının sistem, bilgi ve varlıklarının gizlilik, bütünlük ve erişilebilirlik özelliğini korumak ve uyulması gereken kuralları tanımlamaktır.

2. KAPSAM

Tüm kurum çalışanları, geçici görevliler ve kurumun bilgi varlıklarına erişimine izin verilmiş olan diğer kurum/kuruluş/şirket çalışanları bu politika ile belirtilen kurallara uymak zorundadır.

3. TANIMLAR VE KISALTMALAR

Kurum	Gazi Üniversitesi
BİDB	Bilgi İşlem Daire Başkanlığı
BGYS	Bilgi Güvenliği Yönetim Sistemi
Kullanıcı	Kurumsal Bilgiye Erişen Kişi
Bilgi sistemi	Kurumun sahip olduğu ya da korumakla yükümlü olduğu tüm sunucuları, veri tabanlarını, istemcileri, ağ altyapısını, verileri ve bilgisayar bileşenlerini içerir. Bilgi sistemlerinin kullanımı, aynı zamanda internet erişimi, e-posta hizmeti gibi iç ve dış servisleri de içerir.
Bilgi varlıkları	Bu politika özelinde, bilgi sistemleri, yazılı dokümanlar, donanım, telefonlar, taşınabilir bilgisayarlar, saklanan veri gibi varlıklardır.
peer-to-peer	İki veya daha fazla istemci arasında veri paylaşmak için kullanılan bir ağ protokolüdür.
Tor	Kullanıcılarına anonim iletişim imkânı sağlayan bir ağ ve yazılım projesinin adıdır.
penetrasyon	Penetrasyon Testi kötü niyetli bir saldırgan perspektifinde, hedeflenen sistemlere ve verilere yetkisiz erişim sağlamayı amaçlayan bir saldırı similasyonudur.

4. UYGULAMA

4.1. Genel Hususlar

- Tüm çalışanlar bilgi varlıklarını, kasten veya kazara, yetkisiz erişime, değiştirilmeye, kopya edilmeye, tahrif ve yok edilmeye veya ifşa edilmeye karşı korumakla sorumludur. Tüm personel, kendileri ile ilgili iş verilerinin sahibi olup bu varlıkların korunmasından nihai olarak sorumludur.

- İnternet kaynakları onaylanmamış, ücretsiz veya ticari herhangi bir yazılımın indirilmesi, dağıtılması veya sabit disk, harici disk, USB Bellek, flaş bellek kartları, CD, DVD gibi taşınabilir her türlü kişisel depolama ortamının kuruma girişi ve kullanımı ile ilgili belirlenen kurallara uymakla sorumludur.
- Kuruma ait yazılım ve donanımlar yasa dışı, Kurum politikalarına aykırı veya Kurum çıkarlarına ters düşecek şekilde kullanılamaz.
- İnternet kaynakları onaylanmamış, ücretsiz veya ticari hiçbir yazılımın dağıtılması, indirilmesi veya yüklenmesi için kullanılamaz.
- İnternet dahil Kuruma ait ağlar, Kurum e-posta hesapları, telefon ve bilgisayarlar gibi bilgi işleme imkanları sadece iş amaçlı kullanım içindir. Aksi durumlarda kullanılamazlar. Kullanımdan doğacak zararlardan kullanıcı sorumludur.
- Yeni tedarik edilen veya ağa yeni bağlanacak donanımlar Envanter Yönetim Sistemine kaydı yapılmadan kurum ağına bağlanamaz.
- Gizlilik sınıfı "kişiye özel", "gizli" ve "çok gizli" olan donanım, bilgi ya da yazılım; hangi ortamda bulunursa bulunsun (kâğıt, flash disk, hard disk vs) varlığın kullanıldığı birim yöneticisinin izni olmadan kurum dışına çıkarılmamalıdır.
- Bilgi sistemleri kullanıcıları, sadece varlık sahibi tarafından kendilerine verilen yetkiler dahilinde bilgi varlıklarına erişebilirler.
- Kullanıcılar, erişim yetkilerini sadece yetkinin verilme amacına uygun olarak kullanabilirler.
- Kullanıcılar, güvenlik önlemlerini bypass geçmeye ya da devre dışı bırakmaya yönelik hiçbir girişimin içinde bulunamazlar.

4.2. Kabul Edilebilir Yazılım Kullanımı

- **Kabul Edilebilir Yazılım:** Bilişim sistemleri içerisinde yer alan istemci ve sunucu bilgisayarlar üzerinde kullanılan işletim sistemleri, ofis uygulamaları, güvenlik yazılımları, paket programlar, tüm uygulama ve yönetim yazılımları ile kurum içinde geliştirilen yazılımları kapsar.
- **Kurumsal Kullanım:** Kurumda sadece BİDB tarafından onaylanmış yazılımlar kullanılabilir. Kullanıcılar yazılımlarla ilgili tüm telif hakkı yasalarına uymak zorundadır. Kurum tarafından kullanılan tüm yazılımlar yasal yollardan temin edilmiş olmalı ve sınai mülkiyet düzenlemelerine aykırılık teşkil etmemelidir. Kuruma ait yazılımlar kullanılırken ilgili mevzuat çerçevesinde hareket edilmelidir.
- **Uygunsuz Kullanım:** Kuruma tarafından kullanıcılara sağlanan tüm yazılımlar hiçbir şekilde yasa dışı, kurum çıkarlarıyla çelişecek veya normal operasyon ve iş aktivitelerini engelleyecek şekilde kullanılamaz. Kuruma ait yazılımların izinsiz çoğaltılması yasaktır. Kurum iletişim alt

yapısı ücretsiz, deneme sürümü veya ticari hiçbir yazılımın üreticiler tarafından izin verilenin dışında kopyalanması, gönderilmesi, alınması veya çoğaltılması için kullanılamaz.

- **İzleme:** BİDB' den sorumlu Daire Başkanı tarafından yetkilendirilmiş personel, kullanıcılarının bilgisayarlarında yüklü bulunan veya kullanılan yazılımları herhangi bir zamanda kontrol edebilir. Kurum BİDB tarafından sağlanan yazılımlar kullanılarak yapılan işlemleri kayıt altına alma ve izleme hakkını saklı tutar. Bu bilgiler ilgili yasalar çerçevesinde kullanıcının izni alınmaksızın kanun uygulayıcılar ile paylaşılabilir.

4.3. İnternet Erişim Hizmeti Kullanımı

- **Genel Kurallar:** Kurum internet erişim hizmetinin temel amacı mevcut yasalar çerçevesinde kurum işlerinin yürütülmesi sırasında ihtiyaç duyulan internet erişiminin sağlanmasıdır. Bu sistemlerin yasa dışı, rahatsız edici, kurumun diğer politika, standart ve rehberlerine aykırı veya kuruma zarar verecek herhangi bir şekilde kullanımı bu politikanın ihlal edildiği anlamına gelmektedir.
- **Kurumsal Kullanım:** Kurum tarafından sağlanan internet erişim hizmeti öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılır.
- Kurum çıkarlarıyla çakışmadığı sürece internet erişim hizmetinin kişisel kullanımına BİDB tarafından uygulanan kısıtlamalar çerçevesinde izin verilmektedir.
- Kurum internet kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulur. Kullanıcılar kendi kullanıcı hesaplarıyla internet üzerinde gerçekleştirilen tüm işlemlerden sorumludur. Bunun için kullanıcılar kimlik bilgilerini uygun şekilde saklar ve başkaları ile paylaşmaz.
- **Uygunsuz Kullanımlar:** Kurumun internet erişim hizmeti hiçbir şekilde yasa dışı kullanılamaz, kurum çıkarlarıyla çelişemez ve kurumun normal operasyon ve iş aktivitelerini engelleyemez.
- Kurum kaynakları; uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz.
- Yürürlükteki mevzuata aykırı faaliyetler içerisinde bulunan sohbet gruplarına, forumlara, elektronik haber gruplarına katılmak ve sitelere erişmek yasaktır.
- Kullanıcıların sistemi kullanmak için gerekli kimlik bilgilerini başkalarına vermeleri yasaktır.
- Kurum dışından hiçbir surette port taraması veya ağ taraması yapılamaz. Güvenlik denetimi ve erişim arızalarının tespiti haricinde kurum internet erişim ağının izlenmesi yasaktır.
- Kurum kritik bilgisinin ortaya çıkmasına veya kurum servislerinin ulaşılamaz hale gelmesine neden olacak tüm eylemler yasaktır.
- Kurumsal İnternet erişimi üzerinden iş ile ilgili olmayan (Müzik, video dosyaları) yüksek hacimli dosyalar gönderilemez ve/veya indirilemez.

- Hiçbir çalışan peer-to-peer bağlantı yoluyla internetteki servisleri kullanamaz.
- Çalışanlar, işleri için gereken ancak kurum politikalarına göre engellenmiş Internet sayfaları ya da erişimin engellenmesini gerekli gördükleri Internet sayfaları için yönetici onayı eşliğinde BIDB'ye başvurabilir. Bu talepler değerlendirilerek uygun görülürse işleme alınacaktır.
- Kurumsal İnternet erişimi üzerinden "Tor" ağına bağlantı yapılamaz.
- Kurumsal İnternet erişimi üzerinden genel ahlak anlayışına aykırı internet sitelerine erişilemez ve/veya dosya indirimi yapılamaz.
- Üçüncü şahısların kurumsal interneti kullanmaları BİDB'nin izni doğrultusunda gerçekleştirilir.
- İş sürekliliğinin devamlılığını tehdit edecek herhangi bir bilgi (sistem kullanım şifreleri, güvenlik parametreleri vb.), Internet üzerinden şifrelemeden, okunabilecek bir şekilde gönderilmez. Hassas bilgilerin Internet üzerinden taşınması gerektiğinde, bu bilgiler kesinlikle ek şifreleme mekanizmaları ile korunur.
- **Tarayıcı Yazılımlar:** Kullanıcılar sadece BİDB Grubu tarafından onaylanmış tarayıcı yazılımlarını ve konfigürasyonlarını kullanabilirler.
- Tarayıcı yazılımının mevcut güvenlik ayarları üzerinde kullanıcıların değişiklik yapması engellenir.
- **İndirilen Yazılımlar:** Kurum internet kaynakları BİDB tarafından onaylanmamış, ücretsiz veya ticari hiçbir yazılımın dağıtılması, indirilmesi veya yüklenilmesi için kullanılamaz.
- İndirilen tüm yazılımlar kullanılmadan önce zararlı kodlara ve virüslere karşı taramadan geçirilmelidir.
- **İzleme:** BIDB internet erişim hizmeti kullanılarak yapılan tüm işlemleri kayıt altına alma ve izleme hakkını saklı tutar. Kurum internet erişim hizmeti kullanılarak yapılan işlemlerin günlük kayıtlarını ilgili mevzuat çerçevesinde kanun uygulayıcılarla kullanıcının izni olmaksızın paylaşabilir.

4.4. Sosyal Medya Kullanımı

- Kurum Resmi Sosyal Medya Hesaplarını yönetme, kontrol ve denetim yetkisi ile sorumluluğu Basın ve Halka İlişkiler Müdürlüğüne aittir.
- BİDB Resmi Sosyal Medya Hesaplarını yönetme, kontrol ve denetim yetkisi ile sorumluluğu Bilgi İşlem Daire Başkanlığına aittir.
- Kurum personeli, kuruma ait gizlilik dereceli verileri/belgeleri sosyal medyada paylaşamaz.
- Kurum personeli, departman toplantı içerik, detay ve mekânları sosyal medyada işaretleyemez.

- Kurum personeli sosyal medyada kurumla ilgili gizlilik, güvenlik ve rekabet açısından risk oluşturabilecek uygulamalar kullanılamaz.
- Kurum personeli sosyal medyayı kullanarak öğrencileri, tedarikçileri, çalışanları veya diğer paydaşları aşağılayamaz, rakipler hakkında yanlış veya kanıtlanmamış beyanlarda bulunamaz.
- Kurum personeli kişisel sosyal medya hesaplarından yaptıkları paylaşım ve yorumlardan kişisel olarak sorumludur.
- Kurum faaliyetleri (eğitim, sosyal, kültürel faaliyetler vb.) sırasında çekilen fotoğraf ve videolar sadece kurum resmi sosyal medya hesaplarında paylaşılabilir.

4.5. E-posta kullanımı

- Kurum personeli kurum adına yaptığı tüm elektronik posta (e-mail) haberleşmeleri, kurumsal elektronik posta adresi yoluyla yapar, şahsi e-posta adresleri kurumla ilgili haberleşmelerde kullanılmaz.
- Kurumsal e-posta sistemi ile taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi kesinlikle yasaktır. Bu tür özelliklere sahip bir mail alındığında SOME ekibi ve BGYS birimi haberdar edilir.
- Kurum çalışanları kurumun e-posta sistemini özel işlerinde kullanamaz. Kişisel kullanım için internetteki listelere ve sitelere üye olunması durumunda kurumsal e-posta adresleri kullanılamaz.
- Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul eder. Suç teşkil edebilecek tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden kullanıcı sorumludur. E-posta içerisinde uygun olmayan içerikler (ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderilmesi yasaktır.
- Kurum çalışanları kendilerine ait kurumsal e-posta adresinden gönderilen e-postalardan doğacak hukuki işlemlerden kendileri sorumludur.
- Kurum çalışanları herhangi bir sebepten ötürü başka çalışanların e-posta hesaplarını kesinlikle kullanamaz.
- E-posta hesabına erişim şifreleri kişiye özeldir ve hiçbir surette başkaları ile paylaşılmaz.
- Kuruma ait çok gizli ve hassas bilgiler gönderilen mesajlarda ve/veya eklerinde yer almamalıdır. Gönderilmesi gerektiği durumlar oluştuysa e-postalar şifrelenerek iletilmelidir.
- Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmaz. Bu tür mailler alındığında SOME ekibi ve BGYS ekibi haberdar edilir.
- Kullanıcı, kullanıcı parolası girmesini isteyen e-postaların; sahte e-posta olabileceği dikkate

alarak, herhangi bir işlem yapmadan SOME ekibi ve BGYS ekibini haberdar eder.

- Başkanlık bilgi güvenliği gereksinimleri çerçevesinde gönderilen ve alınan e-posta iletilerini elektronik olarak tarayabilir ve filtreleyebilir.
- Kullanıcı, kurumsal e-postalara kurum iş akışının aksamaması için zamanında yanıt verir.
- Kullanıcı, e-postaların doğru mail adreslerine ve doğru içerikle gönderildiğinden emin olmalıdır.
- Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engeller.
- Gönderilen mesaj başka bir kullanıcıdan gelen mesajın iletilmesi (forward) ile oluşturulduysa, iletilen mesajda yeni alıcıya iletilmesi uygun olmayan bir içerik olmayacak şekilde yeniden düzenleme yapılır.
- Üniversite ağından dış dünyaya gönderilen e-posta mesajları BİDB tarafından belirlenen e-posta tarama ve güvenlik sistemleri ile otomatik bir denetime tabi tutulur. Denetimi geçemeyen e-posta mesajları bloklanır.
- Çalışanlar, gizli ve kuruma özel e-postaları kurum dışındaki üçüncü şahıslar ile hiçbir şekilde ve sebeple paylaşamaz.
- Kaynağı bilinmeyen e-posta ekinde gelen ve virüs, e-mail bombaları ve Truva atı gibi zararlı kodlar içerebilecek dosyalar kesinlikle açılmaz ve derhal silinir.
- Kurumdan ayrılan çalışanın kurumsal e-posta hesabı kapatılır ve/veya yöneticisinden gelen talep doğrultusunda ilgili talepte belirtilen süre için pasif hale getirilir.
- E-posta hesabının parolası belirli zaman dilimlerinde mutlaka sistem tarafından değişmeye zorlanır.
- E-posta ile alınan eklentiler ve önemli içerikler, e-posta hesabına zarar gelmesi riskine karşı, mutlaka uygun başka bir ortama aktarılarak arşivlenmelidir. E-posta hesapları bilgi arşivi olarak kullanılmamalıdır.

4.6. Bilgisayar ve Mobil Cihaz Kullanımı

- Kurum personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş güvenlik cihazlarını korumaktan sorumludur. Erişim bilgileri herhangi birine söylenemez ve bu bilgiler başkaları ile paylaşılamaz.
- Kurum bilgisayarlarına kurumun lisanslı ve güncel işletim sistemleri harici kurulum yapılamaz. Sadece iş için gerektiği durumlarda BGYS ekibine iletilerek bu kurulumlar gerçekleştirilebilir.
- Hiçbir personel, bilgisayarlarından antivirüs koruma yazılımını devre dışı bırakamaz.
- Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.

- Hiçbir personel izin almadan kendi bilgisayarında veya başka bir kaynak kullanarak, BİDB' nin ağını tarayamaz, izleyemez veya dinleyemez.
- BİDB' den onaylı resmi penetrasyon testleri haricinde, BİDB bünyesindeki bilgisayar sunucuları için içeriden veya dışarıdan port taraması yapılması yasaktır.
- Hiçbir personel, Kurum içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.
- Mobil cihazlarda tuş kilidi kullanımı zorunludur.
- Kurumsal uygulamalar dışında cihazlara uygulama yüklenmemelidir.
- Cihazlara yetkisiz erişimlerin engellemesi için kişi yanında bulundurmadığı durumlarda fiziksel kilitli alanlarda tutulur.
- Cihaz parolaları PLK-04-Rev.00-Parola ve Şifreleme Politikası' na uygun olarak belirlenir.
- Cihazlar üzerinden Kurum kaynaklarına erişim gerektiği durumlarda PLK-03-Rev.00-Uzaktan Çalışma Politikası' na uygun olarak erişim sağlanır.
- Cihazlar, zarar veya arızaya sebep olarak dış etkenlerden korunur. Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.
- Mobil cihazlar özellikle dış ortamlarda kullanırken hırsızlık/ kaybolma gibi olaylardan korunmak amacıyla ortada başıboş bırakılmaz. Mobil cihazlar araç içinde görünür şekilde bırakılmaz.

4.7. Taşınabilir Ortamların Kullanımı

- Taşınabilir medya için dosya transferi yapılmadan tüm medya anti virüs programı ile manuel olarak taranır.
- Taşınabilir medya kullanıcılarının anti-virüs yazılımının bilgisayarlarda yüklü ve düzenli çalışıyor olmasından, aksi durumlar için Sistem Yönetim Biriminin bilgilendirme yapılmasından sorumludur.
- Taşınabilir medyalar üzerinde kriptolama yapılmış veya şifrelenmiş formatı bilinmeyen verilerin transferi yasaktır.

4.8. Telekomünikasyon Cihazları Kullanım Politikası

- **Kurumsal Kullanım:** Kurum telekomünikasyon cihazları öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalıdır. Kurum çıkarlarıyla çakışmadığı sürece telekomünikasyon cihazlarının kişisel kullanımına Başkanlık tarafından belirlenebilecek kısıtlamalar çerçevesinde izin verilmektedir. Kurum telekomünikasyon cihazları kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır. Kullanıcılar telekomünikasyon cihazları ile yaptıkları tüm iletişimden sorumludur.

- **Uygunsuz Kullanım:** Kurum telekomünikasyon cihazları hiçbir şekilde yasa dışı kullanılamaz, kurum çıkarlarıyla çelişen işlerde kullanılamaz ve kurumun normal operasyon ve iş aktivitelerini engelleyemez. Kurum telekomünikasyon cihazları uygunsuz içeriği saklamak, erişmek, indirmek ve iletmek için kullanılamaz. Kullanıcıların telekomünikasyon cihazlarını kullanmak için gerekli kimlik bilgilerini başkalarına vermeleri yasaktır.
- **Telefon Sistemi:** Telefon konuşmaları sırasında hoparlörler, ses ve video kayıt cihazları, video konferans ve benzeri cihazlar kullanılmadan önce görüşmede yer alan herkese bildirilmeli ve herkesten izin alınmalıdır. Şehirler ve milletler arası konuşmalar sadece yetkilendirilmiş kullanıcılar tarafından yapılabilir. Kuruma ait hassas bilginin yetkisiz kişilerin eline geçebileceği durumlarda kullanıcılar bu bilgileri telefon görüşmelerinde kullanmamalıdır. Ayrıca bu tip görüşmeler yapılırken kablosuz cihazlar veya cep telefonları kullanılmamalıdır.
- **Fakslar:** Kurum adına gönderilen tüm faksların ilk sayfasında aşağıdaki ifade yer almalıdır:
- *"Bu faks BİDB 'e ait özel, gizli veya telifli bilgi içeriyor olabilir. Bu faks sadece belirtilen alıcı içindir. Eğer bu faksın alıcısı siz değilseniz bu faksın içeriğini okumak, değiştirmek veya kopyalamak yasa dışı olabilir. Eğer bu faks size yanlışlıkla ulaşmışsa, içeriğini hiçbir şekilde kullanmayınız. Bu durumda lütfen faks gönderen kişiye haber veriniz ve tüm elektronik ve yazılı kopyalarını siliniz."*
- **İzleme:** Kurumumuz, telekomünikasyon cihazları kullanılarak gerçekleştirilen aktivitelerle ilgili bilgiyi kanun uygulayıcılarla kullanıcının izni aranmaksızın paylaşma hakkını saklı tutar.

4.9. Yazıcı ve Fotokopi Makinalarının Kullanımı

- Gizlilik dereceli dokümanlar yazdırılırken, bilginin yetkisi olmayan kişiler tarafından görülmesini veya ele geçirilmesini engellemek için yazdırma esnasında yazıcının yanında bulunulmalıdır.
- Orijinal ve kopya doküman nüshaları yazıcı ve fotokopi makinelerinde bırakılmamalıdır. Dokümanlar makinaya sıkışmış olsa da çıkarılmalı ve gerekirse imha edilmelidir.
- Yazıcı ve fotokopi makinalarının kişisel kullanımı sınırlı olmalıdır.

4.10. Basılı Dokümanların Kullanımı

- Gizlilik dereceli dokümanlara sadece yetkili çalışanlar tarafından erişilebilir.
- Gizlilik dereceli dokümanlar zarf ile ve etiketleme yapılarak (Gizlilik İbaresi ile) gönderilir. Bu dokümanlar imza karşılığında teslim alınır ve teslim edilir.
- Gizlilik dereceli dokümanlar yetkisiz erişme karşı korunması için kilitli dolaplar gibi erişim

kontrolü sağlanan ortamlarda saklanır.

5. YAPTIRIM VE CEZA

Tüm kullanıcılar **Varlıkların Kabul Edilebilir Kullanım Politikası** ile birlikte; BGYS kapsamındaki tüm ilgili politika ve prosedürlerdeki kuralları bilmek ve bu kurallara uymaktan, bilgi varlıklarına erişim hakkı istemek için kurum tarafından onaylanmış süreç ve prosedürleri kullanmaktan, şifre, e-imza gibi kurum tarafından verilmiş olan kimlik doğrulama bilgilerini korumaktan, bilgi kendi kullanımındayken bilginin gizliliğini, bütünlüğünü ve erişebilirliğini varlık sahibi tarafından belirlenen önlemlere uygun olarak korumaktan sorumludur. Varlıkların Kabul Edilebilir Kullanım Politikası tarafından düzenlenen kurallara uymayanlara Disiplin Prosedürü çerçevesinde yaptırım ve cezalar uygulanır. Bu cezalar 657 sayılı Devlet Memurları Kanunu ve kişinin bağlı olduğu ilgili diğer mevzuatlara uygun olarak belirlenir.

6. GÖZDEN GEÇİRME VE ONAY

Varlıkların Kabul Edilebilir Kullanım Politikası yılda bir kez BGYS Birimi koordinesinde gözden geçirilir ve varsa değişiklikler Bilgi İşlem Daire Başkanı tarafından onaylanır. Gözden geçirme, Yönetimin Sistemi Gözden Geçirme Toplantısı gündemine alınarak gerçekleştirilir.

7. İLGİLİ DÖKÜMANLAR

- Tüm BGYS Dokümantasyonu