



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	BGYS-PL01
Yayın Tarihi	06.07.2015
Revizyon Tarihi	04.05.2026
Revizyon No	07
Sayfa No	1 / 69



BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI

BİLGİ GÜVENLİĞİ POLİTİKASI

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı

Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	BGYS-PL01
Yayın Tarihi	06.07.2015
Revizyon Tarihi	04.05.2026
Revizyon No	07
Sayfa No	2 / 69

İÇİNDEKİLER

İÇİNDEKİLER.....	2
1. Giriş.....	4
1.1. Amaç	4
1.2. Kapsam.....	5
1.3. Tanımlar	5
1.4. Sorumluluk	5
2. Bilgi Güvenliği Hedefleri ve Prensipleri.....	6
2.1. Görevler Ayrılığı Prensipleri	6
3. Bilgi Güvenliği Organizasyonu ve Altyapısı	7
3.1. BGYS Takımı ve Yetkileri.....	7
<i>BGYS Yöneticisi Görev, Yetki ve Sorumlulukları:</i>	7
<i>BGYS Yönetim Temsilcisi ve BGYS Yönetim Temsilci Yardımcısı Görev, Yetki ve Sorumlulukları:</i>	7
<i>BGYS Takım Üyesi Görev, Yetki ve Sorumlulukları:</i>	8
3.2. BGYS Uygulamalarına Katılım	9
3.3. BGYS Yönetim Gözden Geçirme (YGG) Toplantıları.....	10
4. Risk Analizi ve Yönetim Stratejisi.....	11
4.1. Risk Değerlendirme Metodolojisi	11
4.2. Risk İşleme Metodolojisi	12
4.3. UB01 Uygulanabilirlik Bildirgesi	13
5. Bilgi Hassasiyeti ve Riskler	14
5.1. Bilgi Varlıklarımız	14
5.2. Varlık Sınıflandırması	14
5.3. Kritik Varlıklar.....	17
6. Bilgi Güvenliği Politika, Prosedür ve Rehberleri.....	18
6.1. Bilgi Güvenliği Politikası ve Rehberi	18
6.2. Bilgi Güvenliği Prosedürleri ve Planları	18
7. Bilgi Güvenliği Eğitimleri.....	18
8. Doküman ve Kayıtların Kontrolü.....	18
9. Bilgi Güvenliği İç Denetimleri.....	19
10. Sürekli İyileştirme ve Düzeltici – Önleyici Faaliyetler.....	19
11. Yaptırım	19
12. Bilgi Güvenliği Alt Politikaları	20
12.1. Personel Gizlilik Politikası	20
12.2. Üçüncü Taraf Gizlilik Politikası	24

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı

Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	BGYS-PL01
Yayın Tarihi	06.07.2015
Revizyon Tarihi	04.05.2026
Revizyon No	07
Sayfa No	3 / 69

12.3.	Kurumsal Bilgi Güvenliği Politikası	26
12.4.	Kullanıcı Sorumlulukları Politikası.....	29
12.5.	Varlıklara Yönelik Sorumluluk Politikası	31
12.6.	Kabul Edilebilir Kullanım Politikası	32
12.7.	Bilgi Sınıflandırma Politikası	33
12.8.	Ekipman Güvenliği Politikası	35
12.9.	Zararlı Yazılımlara Karşı Korunma Politikası	37
12.10.	Ağ Erişim Politikası	39
12.11.	Bilgi ve Yazılım Alışveriş Politikası.....	41
12.12.	Bilgi Koruma Politikası.....	44
12.13.	Sunucu Güvenliği Politikası.....	45
12.14.	Parola Koruma Politikası	48
12.15.	Uzaktan Bağlantı Politikası	50
12.16.	Yazılım Geliştirme Politikası	51
12.17.	Erişim Kontrol Politikası.....	54
12.18.	Kimlik Doğrulama ve Yetkilendirme Politikası.....	56
12.19.	Kriptografik Kontrollerin Kullanımı Politikası	57
12.20.	Temiz Masa - Temiz Ekran Politikası.....	59
12.21.	Sosyal Medya Kullanım Politikası	61
12.22.	Anlık Mesajlaşma Güvenliği Politikası.....	63
12.23.	Mobil Cihaz Kullanım Politikası.....	64
12.24.	Kişisel Veri Saklama ve İmha Politikası	66

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı

Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	4 / 69

1. Giriş

BGYS politikası, Kurum bünyesinde yürütülen bilgi güvenliği yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içeren bir rehberdir. Bu politikada tüm çalışanları ilgilendiren maddeler olduğu gibi sadece bazı bölümleri ilgilendiren maddeler de bulunmaktadır.

1.1. Amaç

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır. Bilgi diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat Kurum açısından en önemli varlıklardan biridir. Bilgi güvenliği yönetim sistemimiz ISO 27001:2013 standardına uygun olarak kurulmuş, 2017 ve sonrasında 2022 standardına göre güncellenmiş ve bu standardın gerekliliklerini karşılayacak şekilde PUKÖ (Planla, Uygula, Kontrol et, Önlem al) sürekli iyileştirme döngüsü çerçevesinde bir süreç olarak uygulanmaktadır.

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ve riayeti ile başarılabilir bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden ibaret de değildir. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuda çeşitli kontrollerin risk yönetimi metoduyla seçilmesi uygulanması ve sürekli ölçülmesi demek olan bilgi güvenliği yönetim sistemi çalışmalarımızın genel özeti bu politikada verilmektedir. Uygulama detay bilgileri için sistem dokümantasyonuna, ilgili prosedürlere, rehberlere, planlara ve raporlara bakılmalıdır.

Bu politika bilgi güvenliği politikası ve detaylı kullanım politikalarını da kapsayan bir üst dokümandır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	5 / 69

1.2. Kapsam

Bakanlığımızın BGYS kapsamı; ağ yönetimi, sistem yönetimi ve bilgi güvenliği faaliyetlerini, proje ve karar destek faaliyetleri, yazılım, veri tabanı, veri paylaşımı, teknik destek hizmetleri, idari işler faaliyetlerini ve diğer bilgi işlem faaliyetlerini kapsayacak şekilde hazırlanmıştır.

Adresi: Gençlik ve Spor Bakanlığı Oruç Reis Caddesi No:13 Altındağ/ANKARA

1.3. Tanımlar

BGYS: Bilgi Güvenliği Yönetim Sistemi

Risk Yönetimi: Bilgi güvenliği risklerinin analizi, değerlendirilmesi, işlenmesi ve sürekli iyileştirilmesi amacıyla yürütülen yönetimsel faaliyetler.

Risk Analizi: Tehdit ve iş etkisinin çarpımı olan risk puanının bulunması amacıyla her bir bilgi varlığı için zayıflıkların, tehditlerin, iş etkilerinin bulunması ve hesaplanması çalışması.


Risk Değerlendirme: Risk analizi sonucunda bulunan değerlerin yorumlanması ve derecelendirilmesi.

Risk İşleme: Risk değerlendirme sonuçlarına bağlı olarak kaçınma, kabul, kontrol, transfer seçeneklerinden birinin seçilmesi ve uygulama planı.

1.4. Sorumluluk

Bu politikanın hazırlanması ve yürütülmesinden BGYS Yöneticisi, uygulanmasından tüm Kurum personeli sorumludur.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	6 / 69

2. Bilgi Güvenliği Hedefleri ve Prensipleri

Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri yürütülmektedir. Her bir varlık için risk seviyesini kabul edilebilir risk seviyesinin altında tutmak, kabul edilebilir risk seviyesinin altına inen riskler için de iyileştirme yapılması hedeflenmektedir.

T.C. Cumhurbaşkanlığı, Türk Standartları Enstitüsü (TSE), Bilgi Teknolojileri ve İletişim Kurumu ve ilgili diğer kamu kurumlarının bilgi teknolojileri ile ilgili çıkartacakları düzenlemelere uyulması, TS ISO IEC 27001 uygunluğuna bağlı kalınması, bilgi güvenliği yönetim sürecinin sürekli iyileştirilmesi ve bilgi güvenliği farkındalığı oluşturulması hedeflenmektedir.

2.1. Görevler Ayrılığı Prensipleri

Hata, eksiklik, yanlışlık, usulsüzlük ve yolsuzluk risklerini azaltmak için faaliyetler ile mali karar ve işlemlerin onaylanması, uygulanması, kaydedilmesi ve kontrol edilmesi görevleri personel arasında paylaşılmalıdır. Personel sayısının yetersizliği nedeniyle görevler ayrılığı ilkesinin tam olarak uygulanamadığı durumlarda yöneticilerimiz risklerin farkında olmalı ve gerekli önlemleri almalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	7 / 69

3. Bilgi Güvenliği Organizasyonu ve Altyapısı

3.1. BGYS Takımı ve Yetkileri

BGYS Yöneticisi Görev, Yetki ve Sorumlulukları:

- Politika ve hedeflerin Bilgi Güvenliği Yönetim Sistemi için oluşturulmasını ve kurumumuzun stratejik yönetimi ve iş süreçleri ile uyumlu olmasını sağlamak,
- Bilgi Güvenliği Yönetim Sistemi için ihtiyaç duyulan personel, finans, teknoloji ve bilgi kaynaklarının bulunmasını sağlamak,
- BGYS'nin hedeflenen sonuçları elde etmesi için çalışmak,
- Çalışanları ve ilgili tarafları BGYS'nin etkinliğine katkıda bulunmaları için yönlendirmek ve desteklemek,
- Sürekli iyileştirmeyi teşvik etmek,
- Risk Yönetimi Prosedürüne uygun olarak, riskleri değerlendirmek ve kabul edilebilir risk seviyeleri için kriterler tanımlamak,
- İş Sürekliliği Yönetim Prosedürüne uygun olarak, uygulama ve tatbikatlara aktif bir şekilde katılmak,
- BGYS'nin İç Tetkik Prosedürüne uygun olarak iç denetimlerin yapılmasını sağlamak,
- BGYS'nin YGG Prosedürüne uygun olarak yönetimin gözden geçirmesi toplantılarına başkanlık etmek,
- BGYS Yönetim Temsilcisi, Yardımcısı ve BGYS Takımını atamak ve yetkilendirmek.

BGYS Yönetim Temsilcisi ve BGYS Yönetim Temsilci Yardımcısı Görev, Yetki ve Sorumlulukları:

- TS-EN- ISO 27001 Standardına uygun olarak, BGYS'nin kurulması, uygulanması, devam ettirilmesi ve sürekli geliştirilmesi için çalışmalarda bulunmak,
- BGYS dokümantasyonunu hazırlamak,
- Bilgi Güvenliği İhlal Olaylarını üst yönetim ile birlikte yönetmek,


Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	8 / 69

- BGYS'nin planlandığı ve dokümante edildiği gibi uygulanması için gerekli çalışmaları yapmak,
- BGYS dokümanlarında meydana gelen değişiklikleri izlemek ve tüm taraflara duyurusunu yapmak, yeni düzenlemelerin uygulamasını gerçekleştirmek,
- BGYS'de kullanılacak olan form, plan vb. destek dokümanlarının tasarım çalışmalarını yapmak,
- Problem kayıtları, düzenleyici ve önleyici faaliyetler gibi kritik kayıtların saklanmasında ve elden çıkarılmasında ilgili birimlerle koordinasyonu sağlamak,
- Problem kayıtlarının, düzenleyici ve önleyici faaliyetlerin uygun kanallardan başlatılmasını, yürütülmesini ve izlenmesini sağlamak,
- BGYS performansını izlemek, yorumlamak ve takibini yapmak ve üst yönetime raporlamak,
- Hizmetlerin gerçekleşmesi için kaynak taleplerini gözden geçirmek ve üst yönetime sunmak,
- BGYS planlarını hazırlamak,
- BGYS iç denetiminin gerçekleştirilmesini sağlamak,
- BGYS eğitimlerini plan dâhilinde hazırlamak, gerçekleştirilmesini sağlamak ve değerlendirmek,
- Risk yönetimi için izleme, denetim ve gözden geçirmeleri yerine getirmek,
- Yıllık YGG faaliyetlerini gerçekleştirmek,
- BGYS performans sonuçlarını; yönetimin gözden geçirmesi ve sürekli iyileştirme faaliyetlerine esas olmak üzere raporlamak,
- Belgelendirme firmasıyla dış denetimin gerçekleştirilmesini sağlamak.

BGYS Takım Üyesi Görev, Yetki ve Sorumlulukları:

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	9 / 69

- TS-EN- ISO 27001 standardına uygun olarak, BGYS'nin kurulması, uygulanması devam ettirilmesi ve sürekli geliştirilmesi için çalışmalarda bulunmak,
- BGYS sistemi dokümantasyonunu hazırlanmasına katkı sağlamak,
- İhlal Olaylarını BGYS Yönetim Temsilcisi ve Yardımcısı ile beraber yönetmek,
- BGYS'nin planlandığı ve dokümante edildiği gibi uygulanması için gerekli çalışmalara katılmak,
- BGYS dokümanlarında meydana gelen değişiklikleri izlemek ve yeni düzenlemelerin uygulamasına katkı sağlamak,
- BGYS planlarını hazırlama aşamalarına katılmak,
- BGYS iç denetiminin gerçekleştirilmesini sağlamak ve iç denetime katkı sağlamak,
- Risk yönetimi için izleme, denetim ve gözden geçirmelere katkı sağlamak,
- Yıllık YGG faaliyetlerinin gerçekleştirilmesine katkı sağlamak.

3.2. BGYS Uygulamalarına Katılım

Çalışanların ve ilgili tarafların tamamı bu politikada belirtilen şartlara ve kurallara uymalı, bilgi güvenliği takımının görevlerini yerine getirmesinde yardımcı olmalıdır. Her çalışan yönetimce yayınlanan bu politikada belirtilen amaçlara ulaşmak için yürütülen risk yönetimi çalışmalarına ve bilgi güvenliği rehberinde belirtilen kurallara uymakla sorumludur. Talimatlara ve kontrollere uymayanlara tabi olunan mevzuatın disiplin sürecine göre işlem yapılacaktır.

Her çalışan kendisinin kontrolünde ve yönetiminde olan bilgi varlıklarının kontrolü ve gizliliğinden sorumludur. Bu varlıklara yönelik olarak Bakanlığımız risk yönetimi metodolojisi çerçevesinde gerekli analizlerin yapılmasında ve kontrollerin uygulanmasında her çalışana görev düşmektedir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	10 / 69

Çalışan, uygulanan kontrollerin yeterliliğini, verimliliğini izlemek ve güvenlik ihlal olaylarını, ihlale yol açabilecek tehdit ve zayıflıkları gecikmeden Bilgi İşlem Dairesi Başkanlığına bildirmek zorundadır.


Bilgi güvenliği yöneticilerinin bilgisi olmadan bilgi varlıkları ile ilgili donanımsal, yazılımsal ve fiziksel herhangi bir değişiklik yapılmamalıdır. Yapılması gereken değişiklikler ile ilgili Bilgi İşlem Dairesi Başkanlığına mutlaka haber verilmelidir.

3.3. BGYS Yönetim Gözden Geçirme (YGG) Toplantıları

BGYS takımından katılımcıların da yer aldığı ve üst yönetimin bilgi güvenliğinin uygunluğunu, verimliliğini, risk yönetiminin işlevselliğini, tetkik sonuçlarını, düzeltici ve önleyici faaliyetleri ele aldığı yılda en az bir defa düzenlenen bir toplantıdır. Bu toplantıda yönetim risk kabul kriterlerini ve kaynak ihtiyaçlarını değerlendirir. Çalışmaların ve risk değerlendirme ve işleme faaliyetlerinin verimliliğini inceler.

Bu toplantılarda standarda göre girdi ve çıktılar RPR01 YGG Raporu kullanılarak kayıt altına alınmaktadır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	11 / 69

4. Risk Analizi ve Yönetim Stratejisi

Risk analizi için aşağıdaki metot uygulanmaktadır. Bu faaliyetle ilgili kayıtlar VE01 Varlık Envanteri ve Risk Değerlendirme Listesinde tutulmaktadır.

Kapsam dâhilindeki ve bilgi ile ilişkisi olan her varlığın tespiti için varlık keşif çalışması yapılır. Her kullanıcının sahip olduğu (kullandığı ve yönettiği) varlıklar tespit edilir ve varlıkların sorumluları atanır.


Varlık değerlendirmesi Varlık Değeri Kriterlerine göre yapılır. Her varlık için tehditler ve açıklıklar tanımlanır. Risk hesaplama formülü kullanılarak her bir varlık için var olan risk değeri hesaplanır. Risk değerleri için Risk Değerlerine Göre İşleme Seçeneklerinden uygun olanı seçilir. Kontroller ISO 27001:2022'in Ek-A maddesinden seçilerek uygun olanlar her bir riske atfedilir. Kontrolün nasıl uygulanacağı, kim tarafından uygulanacağı izlenir.

4.1. Risk Değerlendirme Metodolojisi

İş etkisi değerlendirilirken varlığın iş üzerindeki kesinti etkisi, yerine koyma maliyeti, bilginin gizliliği, imaja olan etkisi, yasal ve hukuki yükümlülükler bakımından yaratacağı zarar vb. konular ele alınmalıdır.

Olasılık değeri tespit edilirken zayıflıkların çokluğu ve var olan kontrollerin bu zayıflıkları ne kadar kapatabildiği, saldırgan motivasyonu, tehdit biçiminin uygulanma kolaylığı, bilginin üçüncü taraflar için cazibesi, personelin psikolojisi, uygulamanın hassas ve kontrol edilemeyen (politikaya uymama-kuralın etrafından dolaşma) çalışan davranışı gibi unsurlar değerlendirilmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	12 / 69

Varlığın gizlilik, bütünlük, erişilebilirlik değerlerinin aritmetik ortalaması alınarak varlık değeri hesaplanır. Varlık değeri, olasılık değeri ve etki değeri çarpılarak risk değeri hesaplanır ve risk derecesi belirlenir.

4.2. Risk İşleme Metodolojisi

Risk değerlendirme sonucunda tüm varlıklarla ilgili risk değerleri tespit edilir. Bu değerlendirme sürekli olarak yapısal, organizasyonel ve uygulama değişiklikleri çerçevesinde izlenir ve değişken risk sürekli yeniden hesaplanır. **Risk işleme seçenekleri şunlardır: İşle, Kabul Et, Kaçın, Transfer Et.**

Kabul edilebilir risk seviyesi yönetim tarafından 0-26 puan arası riskler olarak tanımlanmıştır. Tüm varlıklar için hedefimiz riskleri bu seviyeye çekmektir.


Aksi belirtilmedikçe bütün risklerin azaltılması ve kontrol edilmesi birincil aksiyondur. Bazı riskler bu seviyeye çekilemediğinde bunların göze alınması ve riskin kabulü yönetim tarafından yapılabilir.

Uygulama düzeyinde riski azaltamadığımız ve yönetimce kabul edilemez riskler için riskten kaçınma opsiyonu geçerlidir. Riske neden olan uygulamadan vazgeçilmesi ve iş sürecinin ve prosedürünün farklılaştırılması risk işleme seçeneklerinden biridir.

Riskin Birimiz kontrollerini aştığı durumlarda (yangın, deprem, sabotaj, afet, soygun vb) emniyet güçleri, kamu acil durum kurumları, sigorta kurumlarına risk transfer edilir.

Risk işlemede birincil aksiyon kontrollerin seçilmesidir. Kontroller; uygulayıcısının ve bu uygulamayı izleyip ölçecek ilgili amirin görüşlerinin alınması, konuyla ilgili teknik iç-dış

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	13 / 69

uzmanların ve danışmanların görüşlerinin alınması ile seçilir. Seçilen kontroller ISO 27001 Standardının EK-A maddelerinden seçilmeye çalışılır. Burada kontrol amaçları ve kontrollerin ifadesi yer alır. Bu kontrollerin teknik düzeyde nasıl uygulanacağı konu uzmanları ve kontrolü uygulayacak kişilerin seçimiyle oluşturulur. Seçilen en uygun kontrolün maliyeti tespit edilir ve riski azaltılacak varlıkla ilgili yapılan varlık değerlemesi ve iş etkisinden dolayı potansiyel mali zararlar kıyaslaması yapılır. Maliyet fayda analizi sonucu seçilen kontrolün uygulanabilir (feasible) olup olmadığına karar verilir. Uygulanabilir kontroller hayata geçirilir. Uygulanabilir olmayan kontroller için tekrar gözden geçirme yapılarak maliyet fayda dengesi sağlanana kadar araştırma süreci devam eder.

Uygulanan kontrol ile ilgili kayıtlar risk işleme planında belirtilir. Maliyetler ve alınan sonuçlar BGYS toplantılarında görüşülür ve riskin yeni durumda ölçüm sonucu risk işleme planındaki ilgili yere yazılır. Risk puanı kabul edilebilir seviyeye çekilene kadar gerekiyorsa yeni kontroller uygulanır ve ölçümlere devam edilir. Riskin son durumu yönetime onaylatılır ve yönetim tarafından kabul edilen riskler için risk işleme faaliyeti tamamlanmış olur.

Risk işleme sonrası hangi periyotta riskin takip edileceği belirlenir. Bir risk hiç bir zaman tamamen ortadan kalkmaz. Varlık üzerindeki tehditler devamlı değişir ve varlığın iş etkisi de zamanla değişebilir. Bu nedenle periyodik yeniden gözden geçirmeler yapılarak riskin son durumu sürekli ölçümlenir.

4.3. UB01 Uygulanabilirlik Bildirgesi

Risk işleme seçenekleri standardın EK-A bölümünde verilen listeden seçilebilir. Seçilen kontrollerin her birinin seçilme amacı, kontrolün içeriği, kontrolün uygulanma biçimi ve uygulanmıyorsa nedeni kısa adı dokümanda belirtilmektedir. UB01 Uygulanabilirlik Bildirgesi gizli bilgi sınıfındadır ve yalnızca BGYS takımının erişimine açıktır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	14 / 69

5. Bilgi Hassasiyeti ve Riskler

5.1. Bilgi Varlıklarımız

Ağ ve sistem varlık grupları, uygulama varlık grubu, taşınabilir cihaz ve ortam varlık grubu, nesnelerin interneti (IOT) cihazları varlık grubu, fiziksel mekânlar varlık grubu ve personel varlık grubu Bakanlığımız için bilgi varlığı olarak tanımlanmıştır.

5.2. Varlık Sınıflandırması

BİLGİ SINIFLANDIRMA KILAVUZU		Saklanma Yeri Sunucu (PC kullanıcıları için)	Saklanma Yeri Laptop	Saklanma Yeri Dolap
Çok Gizli	Bilmesi gerekenlerin dışında diğer kişilerin bilmelerinin istenmediği ve izinsiz açıklandığı takdirde Devletin güvenliğine, ulusal varlık ve bütünlüğe, iç ve dış menfaatlerimize hayati bakımdan son derece büyük zararlar verecek, yabancı bir devlete faydalar sağlayacak ve güvenlik bakımından olağanüstü önemi haiz mesaj, rapor, doküman, araç, gereç, tesis ve yerler için kullanılır. Bilginin kurum dışına çıkması durumunda çok ciddi büyüklükte kayıplara, zarara ve imaj kayıplarına yol açabilir. Finansal bilgiler, kurum ile ilgili davaların bilgileri, etki alanı yöneticisi şifresi vb.	Harici Disk Klasörleri Gizli bölümü	Harici Disk Klasörleri Gizli bölümü	Yetkililer tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar
Gizli	Kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi veya paylaşılmaması kurum açısından çok önemlidir. Gizlilik ön plandadır. Bilmesi gerekenlerin dışında diğer kişilerin bilmelerinin istenmediği ve izinsiz açıklandığı takdirde Devletin	Harici Disk Klasörleri Gizli bölümü	Harici Disk Klasörleri Gizli bölümü	Yetkililer tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	BGYS-PL01
Yayın Tarihi	06.07.2015
Revizyon Tarihi	04.05.2026
Revizyon No	07
Sayfa No	15 / 69

	güvenliğine, ulusal varlık ve bütünlüğe, iç ve dış menfaatlerimize ciddi şekilde zarar verecek, yabancı bir devlete faydalar sağlayacak nitelikte olan mesaj, rapor, doküman, araç, gereç, tesis ve yerler için kullanılır. Bilginin kurumun dışına çıkması durumunda ciddi kayıplar, zararlar oluşabilir. Bilginin tehlikeye atılması yasal ve mevzuata uygunsuzluk yaratabilir. Hedefler, stratejiler, vb.			
Özel	Sadece birime özel bilgilerdir. Birim çalışanları dışında hiçbir 3. taraf birimin veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır. İzinsiz açıklandığı takdirde, Devletin menfaat ve prestijini haleldar edecek ve ya yabancı bir devlete faydalar sağlayacak nitelikte olan mesaj, rapor, doküman, araç, gereç, tesis ve yerler için kullanılır.	Harici Disk Birim klasörleri	Harici Disk Birim klasörleri	Birimin kilitli dolapları
Hizmete Özel	Kurum çalışanlarının kişisel çalışmaları ile ilgili bilgilerdir. Birim işlevleri için yapılan kişisel çalışmalar burada tutulabilir. PC, Laptop veya Dolaplarda işle ilgili olmayan diğer kişisel bilgiler tutulamaz. Erişilebilirlik ön plandadır. İçerdiği bilgi itibarıyla çok gizli, gizli veya özel gizlilik dereceleri ile korunması gerekmeyen fakat bilmesi gerekenlerden başkası tarafından bilinmesi istenmeyen mesaj, rapor, doküman, araç, gereç, tesis ve yerler için kullanılır. Bilginin kurumun dışına çıkması durumunda göz ardı edilebilir düzeyde kayıp yaşanabilir. Bilginin ifşası kuruma ciddi bir zarar vermez. Bilgiye erişim kurum içerisindeki belirli çalışanlara	Harici Disk	PC harddisk	Çalışma masalarının kilitli çekmeceleri

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı

Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	16 / 69

	açıkır. Organizasyon şeması, süreç dokümanları vb.			
Tasnif Dışı	Bu bilgiler birim çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Birimin kendi içerisinde paylaştıkları bilgiler bu sınıfa girer. İçerdiği konular itibariyle gizlilik dereceli bilgi taşımayan, ancak Devlet hizmeti ile ilgili bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir.	Harici Disk Ortak Dosyalar Klasörü	Harici Disk Ortak Dosyalar Klasörü	Birim kilitli ortak dolapları
Normal	Bu bilgilerin erişilebilirliği önemlidir. Bir gizlilik derecesi olmayıp evrakın gittiği yerde ve başlangıçtaki işlemlerinde belirli şahısların (Amir veya sadece onun yetki verdiği personel) açabileceği, bunun dışında herhangi bir şahıs tarafından açılmayacağını ifade eder.	Harici Disk Ortak Dosyalar Klasörü	Harici Disk Ortak Dosyalar Klasörü	Dolaplar

Kurum içinde her çalışan bu sınıflandırma çerçevesinde kendi kullanımında olan veya kendi ürettiği bilgileri sınıflandırmalıdır. Bu sınıflandırmaya göre halka açık dokümanlar web sitesinde yayınlanan ve işlem için ilgili taraflara verilen kâğıt veya elektronik ortamdaki başvuru formu, şartname vb. bilgilerdir. Birime açık bilgiler, birim içinde sadece çalışanlara açık olan bilgilerdir. Birim dışından yetkisiz kişilerce erişilmemesi gereken bilgilerdir. İç kullanım bilgileri Birim içinde kullanım içindir. Gereksinimlere diğer birimlerle paylaşılması gerekmektedir. Gizli bilgiler en kıymetli ve bütünlüğü gizliliği en kritik olan bilgilerdir. Bu bilgilerin korunması hem iş sürekliliği açısından hem de yasal gereksinimler bakımından önemlidir.


Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	17 / 69

5.3. Kritik Varlıklar

Çalışanlar, ağ ve sistem varlıkları, masaüstü ve dizüstü bilgisayarlar, evrak dolapları ile kuruma ait plan, çizim, rapor, geliştirilen yazılım uygulamaları gibi bilgiler kritik varlıklar olarak değerlendirilmektedir. Bu varlıklar risk yönetiminde ve kontrol seçiminde öncelik verilecek olanlardır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	18 / 69

6. Bilgi Güvenliği Politika, Prosedür ve Rehberleri

6.1. Bilgi Güvenliği Politikası ve Rehberi

Bu dokümanda genel bilgi güvenliği kuralları tanımlanmıştır. Her çalışan bu dokümanda belirtilen kurallara uymakla sorumludur.

6.2. Bilgi Güvenliği Prosedürleri ve Planları

Bakanlığımız bilgi güvenliği politikası kapsamında bilgi işlem süreçlerinin işleyişini anlatan, bilgi yedekleme, ihlal olayı müdahale, iç tetkik, doküman ve kayıtların kontrolü, kullanıcı tanımlama, yedekleme, yedekten geri dönüş planı gibi prosedür ve planlar mevcuttur. İlgili çalışanlar yönetimce tanımlanan ve yayımlanan bu prosedür ve planlara uygun hareket etmelidirler.

7. Bilgi Güvenliği Eğitimleri

Tüm Kurum çalışanlarına bilgi güvenliği bilinçlendirme eğitimleri, bilgi güvenliği yönetim sistemimin gerekliliklerini, amaçlarını, kurallarını ve yaptırımlarını anlatan eğitimler düzenlenmektedir. BGYS takımı üyelerine bilgi güvenliği yönetim sistemi kurulumu ve risk yönetimi eğitimi verilmiştir.


Yönetim, BGYS takımı ve çalışanların bilgi güvenliği konusunda bilinçliliği ve eğitimi için gerekli kaynakları tahsis etmektedir.

8. Doküman ve Kayıtların Kontrolü

BGYS ile ilgili dokümanların hazırlanması, yayımlanmadan önce onaylanması, değişikliklerinin-revizyonlarının takibi, gerekli noktalarda doğru versiyonun ulaşılabilir olması amaçlarını yerine getirecek dokümanter PR01 Doküman Hazırlama ve Kontrol Prosedürü hazırlanmıştır. Dokümanların kontrolü bu prosedüre uygun olarak yapılmaktadır.

Kayıtların kontrolü, saklanması, yedeklenmesi, gerektiğinde tekrar elde edilebilmesini sağlamak amacıyla PR02 Kayıtların Kontrolü Prosedürü hazırlanmış ve uygulanmaktadır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	19 / 69

9. Bilgi Güvenliği İç Denetimleri

Kurulan bilgi güvenliği yönetim sisteminin standarda ve tanımlanan politika ve prosedürlere uygunluğunun tespiti için düzenli olarak gerçekleştirilecek iç tetkikler planlanmıştır. İç tetkiklerin nasıl gerçekleştirileceği PR17 İç Tetkik Prosedüründe tanımlanmıştır ve bu prosedüre uygun olarak düzenli iç tetkikler yapılarak sistemdeki uygunsuzluklar tespit edilmektedir.

10.Sürekli İyileştirme ve Düzeltici – Önleyici Faaliyetler

İç tetkiklerde, ihlal olaylarıyla veya çalışanların kendi gözlemleriyle tespit ettikleri uygunsuzlukların tespitinde ve standarda, politikalarımıza, prosedür ve kurallarımıza uymayan durumların tespitinde ortaya çıkan uygunsuzluğun nasıl giderileceği ve potansiyel uygunsuzlukların henüz ortaya çıkmadan önce nasıl önleneceğine ilişkin PR03 Düzeltici ve Önleyici Faaliyetler Prosedürü hazırlanmış ve uygulanmaktadır. Tüm personel düzeltici ve önleyici faaliyetlere katılmakla sorumludur.

11.Yaptırım

Bilgi Güvenliği Politikası ve kapsamındaki detaylı alt politika maddelerinin ihlali durumunda, PR37 Bilgi Güvenliği Disiplin Prosedürü uygulanır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	20 / 69

12.BİLGİ GÜVENLİĞİ ALT POLİTİKALARI

12.1. Personel Gizlilik Politikası

- 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan kişisel ve özel nitelikli kişisel veriler; usulüne uygun olarak etiketlenmiş olan ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL gizlilik derecesindeki her türlü veri, bilgi ve belge; Kuruma veya hizmet sunulan birime ait özel sırlar, mali bilgiler, çalışan bilgileri, sistem bilgileri ve çalışılan süre içinde derlenen tüm bilgiler, materyaller, programlar ve dokümanlar, bilgisayar sistemleri içerisinde saklanan veriler, donanım/yazılım ve tüm diğer düzenleme ve uygulamalar ile personelin çalışma süresi içerisinde yapmış olduğu işler; açıklanması halinde kişi ve kurumlara maddi veya manevi zarar verme ya da herhangi bir kişi veya kuruma haksız yarar sağlama ihtimali bulunan her türlü bilgi ve belge gizli bilgi olarak tanımlanır.
- Personel, Kurumda uygulanmakta olan Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında yayımlanmış politika, prosedür, süreç ve sözleşmelere uygun davranmalı, bahse konu dokümanlarda belirtilen hususları yerine getirmelidir. Personel, politika hükümlerine uygun davranmaktan, ihlali halinde ise Kuruma ve üçüncü kişilere vereceği her türlü zarardan sorumludur.
- Personel, Kurum tarafından düzenlenen bilgi güvenliği farkındalık eğitimleri ile kişisel verilerin korunmasına ilişkin eğitimlere katılmalı ve bu eğitimlerde anlatılan hususlara riayet etmelidir.
- Personel, Kurum tarafından kendisine teslim edilmiş veya erişim yetkisi verilmiş olan gizli kalması gereken bilgileri, sadece görevi ile ilgili işler için kullanılmalıdır. Bu bilgileri kendi gizli bilgisi gibi koruyup ve bilmesi gereken yetkili kişiler haricinde, hiç kimse ile paylaşmamalıdır. Personel, bilgi paylaşabileceği kişiler konusunda tereddütte kalırsa, bir üst amiri ile irtibata geçerek bu bilgileri kimlerle paylaşabileceğini teyit etmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	BGYS-PL01
Yayın Tarihi	06.07.2015
Revizyon Tarihi	04.05.2026
Revizyon No	07
Sayfa No	21 / 69

- Personel, özel olarak yetkilendirildiği durumlar dışında, hizmet verilen tarafların yetkilileri de dâhil olmak üzere yetkisi olmayan hiçbir kimse ile gizli kalması gereken bilgileri paylaşmamalıdır. Yetkisi olmadığı halde, bulunduğu görev ve makamı kullanarak kendisinden bu bilgileri talep eden kişileri, amirine bildirmelidir.
- Personel, gizli kalması gereken bilgileri hiçbir kişi, grup, kurum veya kuruluşun menfaati için kullanamaz.
- Personel, görevi ile ilgili olsun veya olmasın, edindiği ve gizlilik arz eden her türlü bilgiyi sır olarak saklamak ve bunları üçüncü kişiler ile hiçbir şekilde paylaşmamakla yükümlüdür. Bu yükümlülük, personelin Kurum ile ilişkisinin sona ermesi halinde de süresiz olarak devam eder.
- Personel, görevi nedeniyle edindiği gizli bilgiler hakkında, yasal zorunluluklar ve Kurum tarafından resmi olarak izin verilmesi halleri dışında yazılı veya sözlü açıklama yapamaz.
- Personel, görevi kapsamında erişim hakkının bulunduğu sistemleri ve bilgileri, yetkisi içinde ya da yetkisini aşarak kendisine veya bir başkasına çıkar sağlamak amacıyla kullanamaz.
- Personel, Kurumun bilgisi veya onayı dışında, proje ve faaliyetlerde kullanılan veriler ve sistemler üzerinde, görevin gerektirdiği iş ve işlemler dışında değişiklik yapamaz.
- Personel, hangi amaçla olursa olsun görevi kapsamında edindiği bilgileri, proje ve faaliyetlerde kullanılan çeşitli şekillerde (basılı, dijital, manyetik vb.) bulunabilecek olan verileri yetkisiz ve izinsiz olarak kullanamaz, kopyalayamaz, taşıyamaz ve aktaramaz.
- Personel, Kurum tarafından kendisine verilen bilgisayar, tablet, telefon, taşınabilir medya gibi cihazları sadece göreve yönelik, kurumsal faaliyetler için kullanmalıdır. Yürütülecek adli ve idari soruşturmalar kapsamında olmak şartıyla, söz konusu cihazlar ve personelin kurum bilişim sistemleri üzerinde yapmış olduğu işlemler, personele ayrıca herhangi bir bilgilendirme yapılmaksızın, kontrol edilebilir. Bu cihazlarda,

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı

Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	BGYS-PL01
Yayın Tarihi	06.07.2015
Revizyon Tarihi	04.05.2026
Revizyon No	07
Sayfa No	22 / 69

kurumun bilgisi dışında hiçbir mekanik ya da yazılımsal yapılandırma değişikliği yapamaz.

- Personel, sistemlere erişim için kullandığı kullanıcı adı/parolayı hiçbir şekilde başkaları ile paylaşmamalıdır. Parolasının gizli kalması için gereken tüm tedbirleri almalıdır.
- Personel, Kurum sunucuları üzerinden kendisine tahsis edilen e-imza/mobil imza, kullanıcı adı/parola ve/veya IP/MAC adresini kullanarak gerçekleştirdiği her türlü etkinlikten, kurum bilişim kaynakları kullanılarak oluşturduğu ve/veya kendisine tahsis edilen kurum bilişim kaynağı üzerinde bulundurduğu her türlü içerikten (belge, doküman, yazılım vb.) sorumludur.
- Kurum tarafından kişilere kurumsal kullanım için tahsis edilen kurumsal ve tüzel e-posta hesapları, sadece görevle ilgili kurumsal faaliyetler için kullanılmalıdır. Yürütülecek adli ve idari soruşturmalar kapsamında olmak şartıyla, söz konusu e-posta hesapları, personele ayrıca herhangi bir bilgilendirme yapılmaksızın, kontrol edilebilir. Personel, kendi hesabı kullanılarak gönderilen tüm e-postalardan kişisel olarak sorumludur.
- Kuruma ait gizli kalması gereken bilgiler, veri aktarımı vb. maksatlarla, geçici süre için olsa dahi, Kurum kontrolünde olmayan depolama alanlarında (Örn: Google Drive, iCloud, Yandex Disk, We Transfer, Rapid Share vb.) bulundurulmamalıdır. Bu bilgiler mobil uygulamalar (Örn: WhatsApp, Messenger, Line, Viber, Telegram, WeChat, Skype, SnapChat vb.) ve sosyal medya platformları (Örn: Facebook, Youtube, Instagram, Twitter, LinkedIn vb.) üzerinde işlenmemelidir. Personelin şahsi e-posta hesapları üzerinden aktarılmamalıdır.
- Personel, sosyal medya hesaplarını kullanırken görevinin gerektirdiği dikkat ve özeni göstermelidir. Kurumları ve kişileri zor durumda bırakabilecek paylaşımlar yapmaktan kaçınmalıdır.


Hazırlayan: BGYS Yönetim Temsilci Yardımcısı

Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	23 / 69

- Personel, kendi kusuru nedeniyle parolasının ifşa olması durumunda, başkası tarafından yapılmış olsa dahi, teslim edilen kullanıcı adı ve parolalar ile yapılan iş ve işlemlerden şahsen sorumludur.
- Personel, bilgi güvenliği ihlal olaylarını 24 saatten geç olmamak üzere en kısa sürede hemen bir üst amire yazılı yollarla bildirmelidir. Bildirimin geç yapılması nedeniyle veri koruma mevzuatında öngörülen 72 saatlik süreye riayet edilmemesi durumunda personelin idari sorumluluğu doğar.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	24 / 69

12.2. Üçüncü Taraf Gizlilik Politikası

Üçüncü Taraf; tedarikçiler, bayiler, yetkili satıcılar, hizmet sağlayıcıları, danışmanlar, şahıslar gibi her türden iş ilişkisi kurulan kişi, kurum ve topluluklardır.

- Tedarikçilerin finansal durumu senelik olarak gözden geçirilmelidir. Bazı sektörlerde, iflas, bataklık, dolandırıcılık gibi olaylar çok sık gerçekleşmektedir.
- Birim dışından gelen bakım ve tamir çalışanları, diğer tedarikçilerde de olduğu gibi, birim içinde olduğu süre boyunca bir dış taraf taahhünamesi imzalamalıdır.
- Birim içinde kullanılan telefon rehberleri üçüncü tarafların eline geçmemelidir. Sadece uygun, yetkileri almış olan çalışanların organizasyonun bilgi veya iletişim sistemlerine erişimi olmalıdır. Üçüncü taraflardan temin edilen e-posta hizmetlerinin güvenliği garanti altına alınmalıdır.
- Üçüncü taraflarla herhangi bilgi alışverişi yapılmadan önce bir dış taraf taahhünamesi yapılmalıdır.
- Üçüncü taraflara birimin ağına erişim izni verilmeden önce, üçüncü taraf çalışanlarının bilgisayarları ağ güvenliğe dahil edilmelidir. Birim, üçüncü taraflara herhangi bir uyarıda bulunmadan ağa olan erişimlerini kesebilmelidir.
- Anlaşma sona erdiğinde; tarafların, dokümanlarını karşılıklı olarak geri vermesi gerekir.
- Birimin isminin halka yayınlanacak dokümanlarda kullanılabilmesi için üçüncü tarafların uygun kişiler tarafından yetkilendirilmesi gerekir.
- Gizli bilgilerin dağıtımını içeren kurallar belirlenmeli ve üçüncü taraflara bu bilgiler iletilmeden önce taraflarla bu kurallar hakkında anlaşılmalıdır.
- Sanallaştırma hizmetinin üçüncü taraflar aracılığıyla sunulması durumunda, sanallaştırma ortamının güvenliği garanti altına alınmalıdır. Kurumların siber olay yönetimi kapsamındaki hizmetleri üçüncü taraflardan alması durumunda hizmetin güvenliği garanti altına alınmalıdır.
- İş sürekliliği planları kapsamında; hizmet alınan üçüncü tarafların rol ve sorumlulukları


Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	25 / 69

ile birlikte tedarik edilen hizmetlerin süreklilik kriterleri de dikkate alınmalıdır.

- Kurum içerisinde barındırılmayan üçüncü taraf bir uygulama kullanılacak ise uygulama açık kaynak kodlu olmalıdır.
- Kurumun bilgi güvenliği gereksinimleri göz önünde bulundurularak üçüncü taraflar ile yapılan demo ve kavram ispatı (PoC) çalışmalarında, üçüncü tarafın sorumluluklarını içeren gizlilik taahhünamesi hazırlanmalı ve imza altına alınmalıdır. İlgili taahhüname içeriği periyodik olarak gözden geçirilmelidir.
- Güvenli alanlara veya kritik bilgi işleme ortamlarına; destek, bakım gibi hizmetler için gelen üçüncü taraf personeline, yetkili kurum personeli nezaretinde sınırlandırılmış şekilde erişim izni verilmelidir. Ziyaretçilere yönelik; ad, soy ad, geliş amacı ve tarihi, refakat eden personel, giriş/çıkış saat bilgilerini içeren kayıt tutulmalıdır.
- KVKK kapsamında ilgili kişi tarafından talep edilen; güncelleme, anonimleştirme, silme, yok etme işlemleri gerçekleştirilmelidir. Talep edilmesi durumunda bu işlemler kişisel verinin aktarıldığı üçüncü taraflara da iletilmelidir. Yapılacak işlemlerle ilgili bilgilendirme Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e uygun olarak gerçekleştirilmelidir.
- Üçüncü taraflardan temin edilen/hizmet alınan BT ürünlerine, BT hizmetlerine, dış kaynaklı iş süreçlerine, yardım masalarına, çağrı merkezlerine, ara bağlantılara, ortak tesislere vb. yönelik güvenlik gereksinimleri sözleşmelerde detaylı olarak ele alınmalıdır.
- Tedarik edilen veya hizmet alımı ile geliştirilen uygulamalar için yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) içermediğine/içermeyeceğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhüname alınmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	26 / 69

12.3. Kurumsal Bilgi Güvenliği Politikası

- Bilgi güvenliğinden kapsam dâhilindeki bütün personel sorumludur.
- Güvenliği yönetmek ve yönlendirmek için Birimimiz BGYS Ekibi oluşturulmuştur. BGYS Ekibi düzenli olarak yılda bir kez toplanır.
- BGYS Politika ve Prosedürleri, özel durumlar haricinde her yıl gözden geçirilmelidir.
- Bilgi Güvenliğinde; bilgi işlenirken, iletilirken ve muhafaza edilirken Gizlilik, Bütünlük ve Erişilebilirlik esas alınmalıdır.
- Birim kaynak ve bilgilerine erişimde, erişilen kaynak ve bilgi hakkında daha önceden bilgi sahibi olunmalıdır. Hakkında bilgi sahibi olunmayan verilere erişilmemelidir. Bilgisi hakkında tereddüde düşülen konularda bilgi sahiplerine danışılmalıdır.
- Birimin tüm kritik bilgi varlıkları (donanım, yazılım, cihaz, veri) tanımlanmalı ve uygun şekilde koruma altına alınmalıdır.
- Birimin tüm bilgi varlıklarının envanteri çıkarılmalıdır. Tüm bilgi varlıkları uygun şekilde sınıflanıp Birimin iş ihtiyaçları göz önüne alınarak kayıtları tutulmalı, fiziksel varlıklar kategorilerine göre etiketlenmelidir.
- Personelin, yetkisinin olmadığı bilgi varlıklarına erişimi yasaktır.
- Bilgi varlıkları, iletilirken ve taşınırken güvenliği için gerekli tüm önlemler alınmalıdır.
- Birim içinde kullanılacak tüm yazılımlar, gerçek ortama taşınmadan önce uygun güvenlik denetimine tabi tutulmalıdır.
- Birimin yönetimi, kullanılan ortama bakılmaksızın tüm bilgi trafiğini izlemeye yetkilidir.
- Bilişim ağının sınırları Başkanlıkça uygun donanım ve yazılım kullanılarak koruma altına alınıp, periyodik olarak izlenmelidir.
- Bilişim ağına karşı yapılacak saldırılardan korunmak için uygun güvenlik önlemleri alınmalıdır.
- Elektronik ortamda oluşan tüm güvenlik ihlalleri, Birimimiz BGYS Yöneticisine


Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	27 / 69

bildirilmek zorundadır. BGYS Yöneticisi, bu güvenlik ihlallerinin gelecekte tekrar oluşmaması ve kısa zamanda çözümlenmesi için gerekli tedbirleri almalıdır.

- İş sürekliliğinin sağlanması için gerekli önlemler alınmalıdır.
- BGYS Ekibi tarafından Kurum personeli için uygun Bilgi Güvenliği Farkındalık eğitimleri planlanmalı ve uygulanmalıdır.
- Fiziksel güvenliğe önem verilmelidir. Bu nedenle, giriş çıkış kapıları, çalışma odaları ve ürün teslim alma/verme alanları (depolar, giriş kapıları vb) güvenli konuma getirilmeli ve ilgili prosedürler oluşturulmalıdır.
- Birim içinde beklenmedik güvenlik olaylarını yönetmek için BGYS Ekibi gerektiğinde “Güvenlik Kriz Masası” oluşturmalıdır.
- Kuruma ait gizli bilgilerin umuma açık mekânlarda tartışılması, kimliği doğrulanamayan şüpheli kişilere verilmesi ve aktarılması yasaktır.
- Toplantılar sona erdiğinde kullanılan yazı tahtası temizlenmeli, ilgili belge ve not kâğıtları masadan kaldırılmalıdır. Toplantı odalarına Birimimiz personeli harici kişilerin Birimimiz personeli refakati olmaksızın girmemesi sağlanmalıdır.
- Çalışanların gizli bilgi, dosya ve kâğıtları açıkta bırakmaları yasaktır.
- Bilgisayar sistemlerinin Güvenlik Denetimi her yıl ISO27001 standartlarına uygun olarak yapılmalıdır.
- Uzaktan çalışma faaliyetlerinde, çalışma dosyalarını paylaşmak için kurumsal kaynaklar kullanılmalıdır. Kurumsal merkezi kimlik yönetim ve doğrulama sistemleri kullanılmalı veya e-Devlet sistemi ile entegrasyon sağlanmalıdır.
- Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda bulundurulmamalıdır.
- Onarım/tadilat için üçüncü kişilere (yetkisi servis vb.) verilecek cihazlar fabrika ayarlarına döndürülmeli ve içindeki kurumsal veriler silinmelidir. Cihaz içindeki veri silinemeyecek durumda ise cihaz imha edilmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	28 / 69

- Kritik veriye erişen kişisel ve kurumsal cihazlar uzaktan yönetilebilmeli, cihazlara güvenlik politikaları uygulanabilmeli ve gerek duyulduğunda politikalar uzaktan güncellenebilmelidir.
- Kurumsal haberleşme amacıyla sunucuları kurum kontrolünde olan mesajlaşma uygulamaları kullanılmalıdır. Kurumun kendine ait bir haberleşme uygulaması yoksa mesajlaşma amacıyla sunucuları yurt içinde bulunan yerli ve milli uygulamalar tercih edilmelidir.
- Bulut ortamına doğru veri iletimi sağlanırken iletimin tek yönlü olması sağlanmalı, kurumsal ağ bulut ortamından gelecek tehditlere karşı izole olmalıdır.
- Kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapılmamalı, kurumsal e-postalar şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmamalıdır.
- Kurum personeli, T.C. Devletin kabul ettiği bilgi güvenliği ile ilgili ulusal ve uluslararası kanunların dışındaki bir aktivitede bulunmamalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	29 / 69

12.4. Kullanıcı Sorumlulukları Politikası


- Herhangi bir konu veya işi, görev ve sorumlulukları gereği; öğrenme, inceleme, gereğini yerine getirme ve koruma sorumluluğu bulunanlar yetkileri düzeyinde bilgi sahibi olmalıdır.
- Kullanıcıların tahmin edilebilir parolalar kullanılması engellenmelidir. Parola kalitesinin sağlanmakta olduğundan emin olabilmek için bir sistem oluşturulmalıdır. Parolalar belirli aralıklarla değiştirilmeye zorlanmalıdır.
- Personel kullandığı her sistemde farklı bir parola kullanmalıdır.
- Parolalar kullanılmakta olan sistemlerden uzak bir yerde tutulmalıdır. Kullanıcılar parolalarını kâğıda yazmamalıdır.
- Kurum personeli kendi adına tanımlanmış olan kullanıcı adı ve parolası olmadan bilgisayar kullanamaz. Kullanıcılar kendi kullanıcı adlarından sorumludurlar ve kendilerine sistem yöneticisi tarafından atanmış olan kullanıcı adlarını kullanabilirler.
- Kullanıcı hesapları, isimleri ve parolaları, sahipleri dışında başka kimselerce kullanılmamalıdır.
- Personel ve yüklenicilerin kurum varlıklarına erişimi sağlanmadan önce, kendileriyle yapılan sözleşmelerde bilgi güvenliği sorumlulukları belirtilmelidir.
- Kurum personeli tarafından gerçekleştirilen işin tanımı ve gereklilikleri göz önünde bulundurularak, ilgili personelin kurum bünyesindeki bilgi güvenliği rolü, sorumlulukları ve sahip olması gereken asgari yetkinlikler tanımlanmalı ve yazılı hale getirilmelidir.
- Siber olaylar, iş sürekliliği ve felaket kurtarma planlarının devreye alınması aşamasında yer alacak tüm paydaşların ve süreç içinde yer alacak personelin görev ve sorumlulukları dokümante edilmeli ve ilgili taraflara bildirilmelidir.
- İstihdam sorumlulukları değişen personel/yükleniciye yeni bilgi güvenliği sorumlulukları ve görevleri; istihdamı sonlandırılan personel/yükleniciye ise istihdamın sona ermesinden sonra devam edecek bilgi güvenliği sorumlulukları bildirilmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	30 / 69

- Bilgi İşlem Dairesi Başkanlığı tarafından personelin kişisel bilgisayarlarında bulunan verilerin yedeklenmesi yapılmamaktadır. Kişisel bilgisayarında veya depolama alanlarında bulunan dosyalar personelin kendi sorumluluğundadır.
- Yazıcı kullanımı sırasında evrak gizliliği personelin kendi sorumluluğundadır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	31 / 69

12.5. Varlıklara Yönelik Sorumluluk Politikası

- Her yıl bir bilgi varlıkları envanteri yapılmalı ve bu konuda görevlendirilmiş kişiye bu liste verilmelidir. Bu çalışmanın amacı Kurum bilgi varlıklarını tespit etmek ve bu varlıkların kaybedilmesinin engellenmesini sağlamaktır.
- Kurum içinde geliştirilmiş sistem ve yazılımların da Varlık Envanterine eklenmesi gerekir. Bu liste her sene gözden geçirilmelidir.
- Birimin sahip olduğu tüm sistemleri yönetebilecek, kullanıcı ayrıcalıklarını takip edecek ve erişim kontrol logunu izleyecek bir BGYS Yöneticisi belirlenmelidir. BGYS Yöneticisinin birimde bulunamayacağı durumlarda, bu görevi yerine getirebilmesi için BGYS Yönetim Temsilcisini görevlendirmesi gerekir.
- Satın alınacak herhangi bir yazılım veya donanımın bilgi güvenliği standartları ile uyumlu olması gerekir.
- Veri saklama, işleme ve iletme yeteneği olan tüm donanımların güncel bir envanteri tutulmalı, yalnızca yetkilendirilmiş personelin varlık envanterine erişimi mümkün kılınmalıdır.
- Yeni tedarik edilen ya da ağa yeni bağlanacak donanımların, donanım varlık envanterine kaydı yapılmadan kurum ağına bağlanmamasına yönelik politika ve prosedürler oluşturulmalı ve uygulanmalıdır. Donanım envanter içeriğinde yapılan değişiklikler kayıt altına alınmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	32 / 69

12.6. Kabul Edilebilir Kullanım Politikası

- Güvenlikten; Kurum personeli, Kuruma iş yapan yüklenici firmalar her gün sorumludur. İlgili tüm personel, kendi alanlarına ait Güvenlik Politikalarına uymak zorundadır.
- Kurum, veri merkezinde tutulan ve iletilen tüm bilgileri izleme ve denetleme hakkına sahiptir.
- Kurumun gizli olarak belirlediği tüm bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. İş gereksinimi dışında bu bilgilerin kopya edilmesi ve iletilmesi yasaktır.
- 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 paylaşamaz.
- Hiçbir personel, bilgisayarlarından anti virüs koruma yazılımını devre dışı bırakamaz.
- Kaynağı belli olmayan ve üretici firma tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.
- Hiçbir personel izin almadan kendi PC' sinden veya başka bir kaynak kullanarak, kurum bilişim ağını tarayamaz, izleyemez veya dinleyemez.
- Hiçbir personel, birim içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 <p>BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI</p>	<p>BİLGİ GÜVENLİĞİ POLİTİKASI</p>	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	33 / 69

12.7. Bilgi Sınıflandırma Politikası

- Tehlike arz eden herhangi bir ürün veya hizmet, bu tehlikenin doğasını açıklayacak biçimde işaretlenmelidir.
- Her bilginin türünü gösteren işaretlemeler kullanılmalıdır. Bu işaretleme dili tüm personel tarafından bilinmelidir.
- Bir depolama ortamının çeşitli seviyelerde gizlilik içermesi durumunda, en yüksek gizlilik seviyesi içeren bilgiler öncelikli olarak kabul edilmelidir.
- Bilginin gizliliği hangi seviyede olursa olsun, ilgili yöneticilerin bu bilgiye ulaşımı mutlaka olmalıdır.
- Bilgiye atanan gizlilik seviye sınıflandırması senede en az bir defa gözden geçirilmelidir.

Bilgi Sınıfı	Açıklama
ÇOK GİZLİ	Bilmesi gerekenlerin dışında diğer kişilerin bilmelerinin istenmediği ve izinsiz açıklandığı takdirde Devletin güvenliğine, ulusal varlık ve bütünlüğe, iç ve dış menfaatlerimize hayati bakımdan son derece büyük zararlar verecek, yabancı bir devlete faydalar sağlayacak ve güvenlik bakımından olağanüstü önemi haiz mesaj, rapor, doküman, araç, gereç, tesis ve yerler için kullanılır. Bilginin kurum dışına çıkması durumunda çok ciddi büyüklükte kayıplara, zarara ve imaj kayıplarına yol açabilir. Finansal bilgiler, kurum ile ilgili davaların bilgileri, etki alanı yöneticisi şifresi vb.
GİZLİ	Bilmesi gerekenlerin dışında diğer kişilerin bilmelerinin istenmediği ve izinsiz açıklandığı takdirde Devletin güvenliğine, ulusal varlık ve bütünlüğe, iç ve dış menfaatlerimize ciddi şekilde zarar verecek, yabancı bir devlete faydalar sağlayacak nitelikte olan mesaj, rapor, doküman, araç, gereç, tesis ve yerler için kullanılır. Bilginin kurumun dışına çıkması durumunda ciddi kayıplar, zararlar oluşabilir. Bilginin tehlikeye atılması yasal ve mevzuata uygunsuzluk yaratabilir. Hedefler, stratejiler, vb.
ÖZEL	İzinsiz açıklandığı takdirde, Devletin menfaat ve prestijini haleldar edecek ve ya yabancı bir devlete faydalar sağlayacak nitelikte olan mesaj, rapor, doküman, araç, gereç, tesis ve yerler için kullanılır.
HİZMETE ÖZEL	İçerdiği bilgi itibarıyla çok gizli, gizli veya özel gizlilik dereceleri ile korunması gerekmeyen fakat bilmesi gerekenlerden başkası tarafından bilinmesi istenmeyen mesaj, rapor, doküman, araç, gereç, tesis ve yerler için kullanılır. Bilginin kurumun dışına çıkması durumunda göz ardı edilebilir düzeyde kayıp yaşanabilir. Bilginin ifşası kuruma ciddi bir zarar vermez. Bilgiye erişim kurum içerisindeki belirli çalışanlara açıktır. Organizasyon şeması, süreç dokümanları vb.
TASNİF DIŞI	İçerdiği konular itibarıyla gizlilik dereceli bilgi taşımayan, ancak Devlet hizmeti ile ilgili bilgi,

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	BGYS-PL01
Yayın Tarihi	06.07.2015
Revizyon Tarihi	04.05.2026
Revizyon No	07
Sayfa No	34 / 69

	belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir.
NORMAL	Bir gizlilik derecesi olmayıp evrakın gittiği yerde ve başlangıçtaki işlemlerinde belirli şahısların (Amir veya sadece onun yetki verdiği personel) açabileceği, bunun dışında herhangi bir şahıs tarafından açılmayacağını ifade eder.

- Kullanılan çeşitli dosya tiplerinin birbirlerinden ayırt edilebilmesi için dosya isimlendirme hakkında bir sistem oluşturulmalıdır.
- Tüm veri sınıflandırma etiketleri, EBYS etiketleme sistemi ile uyumlu olmalıdır. Kurum içerisinde 6 farklı tip sınıflandırma kullanılır. Çok Gizli, Gizli, Özel, Hizmete Özel, Tasnif Dışı, Normal sınıflandırma seviyesine sahip olan fiziksel ve elektronik bilgiler etiketlenmelidir.
- EBYS’de sadece Hizmete özel sınıflandırması yapılmalıdır. Gizli ve Çok Gizli bilgiler fiziksel olarak oluşturulup kapalı zarflar ile iletilmelidir.
- Kâğıt olarak kopyası saklanan ve sınıflandırılmış olan her sır, gizli bilginin sayfa düzeninde gizlilik seviyesi hakkında gerekli bilgileri içermesi gerekir.
- Gizlilik içeren bilgilerin iletişimi hakkındaki her türlü bilgi taahhütlü yollanmalıdır.
- Alıcılar, gizli bir bilgi alır almaz; kendilerine bu konuda bilgi veren bir yazı iletilmelidir.
- Dış kaynaklardan elde edilen tüm bilgiler, bilgisayar depolama ortamı dâhil, uygun biçimde tüm kurumda kullanılan sınıflandırma sistemi göz önünde bulundurularak etiketlenmelidir.
- Bir bilginin gizli olduğuna karar verilirse, bilginin gizlilik seviyesine göre görünebilir bir yerine uygun etiketler konulmalıdır.
- Gizli bilgiler içeren bir dokümanın içeriğini değiştiren kişi, uygun sınıflandırma etiketlemesini kullanmalıdır.
- Gizli bilgiler, sadece yetkili bilgi sahibi tarafından kopyalanmalıdır. Kopyalama işlemini yürüten kullanıcı, fotokopi makinesinde bırakmış olduğu dokümanlardan sorumludur.
- Kağıt olarak kopyası saklanan ve sınıflandırılmış olan her evrak, elektronik ortamdaki orjinal haliyle aynı gizlilik ibarelerini içermelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	35 / 69

- Resmi yazışmalar, kurumun resmi yazışma platformu olan EBYS de arşivlenmelidir.

12.8. Ekipman Güvenliği Politikası

- Bilgi sistemlerinin üretimine ilişkin tüm tesis ve ekipmanların çevresel koşulları kontrol altında olan güvenli ortamlara yerleştirilmesi gerekir.
- Bilgisayar ve iletişim araçları gibi ekipmanların, üçüncü tarafların erişebileceği noktalardan uzak tutulması gerekir.
- Elektrik kablolarının ve iletişim hatlarının montajı ve bakımı yetkili ve sertifikalı kişiler tarafından yapılmalıdır.
- Tedarikçiler tarafından yapılan tamir ve bakım faaliyetleri yetkili kişiler tarafından yapılmalıdır. Yetkisi olmayan çalışanların bu tip faaliyetleri yürütmesi yasaktır.
- Depolanmış verileri içeren yazılım ve donanım ürünlerinin uygun biçimde muhafaza edilmesi ve çalışır halde kalması için uygun biçimde saklanması, konfigürasyonunun yapılması gereklidir.
- Birim dışından ekipman getirmek isteyen çalışanların öncelikle yöneticilerinden izin alması gerekir.
- Çeşitli bileşenler bilgi sisteminden çıkartılmadan önce, bileşenlerdeki kayıtlı bilgilerin yedeklenmesi, depoya kaldırılması veya imha edilecek bileşenden silinmesi gerekir.
- Önemli bilgi işlem uygulamalarının, çevresel risklerin (yangın, sel, fırtına) azaltıldığı noktalara yerleştirilmesi gerekir. Veri işleme ekipmanlarının yer seviyesinden yukarıda ve nehir, ırmak, kanalizasyon, su rezervuarı ve su borularından uzak bir noktaya yerleştirilmesi gerekir.
- Elektronik alım satım ve finansal sistemlerin güvenli bir şekilde izole edilmiş olması istenir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	36 / 69

- Kurum personeli, uzaktan çalışma faaliyetlerinde yalnızca kurum tarafından sağlanan ve/veya yapılandırma ayarları kurumun bilgi güvenliği gereksinimlerine uygun olan cihazları kullanmalıdır.
- Elektrik, su, gaz ve diğer destekleyici altyapı hizmetlerini kesmek için kullanılan acil durum anahtarları ve vanalar acil çıkışların veya ekipman odalarının yakınında konumlandırılmalıdır.
- Güvenlik ve iş sürekliliği gereksinimlerini sağlamak amacıyla altyapıda yer alan ekipmanlara ait arıza sinyallerinin izlenmesi için alarm mekanizması kurulmalıdır.
- Haberleşme sistemlerinde kullanılan ekipmanı, çevresel tehditler ile enerji destek sistemlerinden kaynaklanacak olumsuz etkilere karşı korumak amacıyla gerekli önlemler alınmalıdır.
- Bilgi işlem merkezlerinin yangın, sudan gelebilecek zararlar ve izinsiz girme gibi durumlardan korunabilmesi için yeterli güvenlik sistemlerine ihtiyacı vardır. Meydana gelen tüm olayların kayıt edildiği bir alarm ve bir raporlama sistemi bulunmalıdır.


Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	37 / 69

12.9. Zararlı Yazılımlara Karşı Korunma Politikası

- İstemci ve sunucu sistemlerinin tamamında zararlı yazılımdan korunma uygulamaları kullanılmalı ve zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanmalıdır. Zararlı yazılımdan korunma uygulamalarına ait politikalar merkezi olarak yönetilmelidir.
- Sistemde düzenli olarak zafiyet taraması yapılmalı ve bu zafiyetlerin yönetimi gerçekleştirilmelidir. Sistem zararlı yazılımlara karşı düzenli olarak taranmalıdır.
- Personelin beyaz listede bulunan uygulamalar haricinde uygulama kurması engellenmelidir.
- Kurumdaki tüm bilgisayarlar, taşınabilir diskleri otomatik olarak zararlı yazılım taramasından geçirecek şekilde yapılandırılmalıdır.
- Zararlı yazılımlardan korunma uygulaması üretici veya ilgili kurum tarafından önerilen şekilde yapılandırılmalı ve güncel tutulmalıdır.
- Tüm zararlı yazılım tespitleri, merkezi yönetim ve kayıt sunucularına iletilmelidir.
- Kurum politikasına uymayan cihazlara bağlantı izni verilmemelidir.
- Zararlı yazılımları tespit eden ve önleyen güvenlik uygulamaları kullanılmalıdır.
- Zararlı yazılımdan korunma uygulamaları kullanılmalı, dosya bütünlüğünü izleyecek ve kayıt tutacak mekanizmalar devreye alınmalıdır.
- Bir virüsün varlığından şüphelenen bir kullanıcı; ilgili bilgisayarı kapatmalı, bilgisayarın ağ bağlantısını kesmeli, bu bilgiyi bilgi güvenliği yöneticisine iletmelidir.
- Her iş istasyonuna antivirüs programı yüklenmelidir. Böylece; Antivirüsler daha hızlı gözlemlenebilecek, şifrelenmiş virüs tanımlamaları, bir önceki kontrolde tanımlanacak, Antivirus başarısızlıkları tesadüfi olacaktır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	38 / 69

- Dış kaynaklı dokümanlar, diğer dokümanların bulunduğu ortama aktarılmadan önce en güncel virüs tanımlamalarını içeren bir antivirüs programı ile taranmalıdır. Eğer doküman şifrelendirilmişse, doğrulanmadan önce şifresi kaldırılmalıdır.
- Yedek alınan dokümanların kopyası bir iş istasyonuna veya server'a kopyalanmadan önce bir antivirüs programı ile taranmalıdır.
- Dosyalar bir üçüncü tarafa gönderilmeden önce virüs taramasından geçirilmelidir.
- Kullanıcılar, mevcut bilgi sistemlerinin normal işleyişine zarar verebilecek, kopyalanmasına neden olacak kodlar yazmamalı, yaymamalı veya yönetmemelidir.
- Kuruluşa ait olmayan sitelerden hiçbir yazılım indirilmemelidir. Dış bir kaynak aracılığı ile indirilen bu tip programlar, yazılım uyumsuzluğuna, diskteki boş alanın kaybına, çalışan verimliliğinin azalmasına, bilgisayarlara virüs, worm veya trojan horse bulaşmasına neden olabilir.
- Dış kuruluşlardan elde edilen yazılımlar, kullanılmadan önce ağa bağlı olmayan bir bilgisayarda güncel bir antivirüs programı ile taranmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	39 / 69

12.10. Ağ Erişim Politikası


- Ağ Yönetim Şubesi personeli, diğer kullanıcıların yetkilendirmesini ve erişim kurallarının uygulanmasını sağlar. Birimimiz ağ yapısı içerisindeki noktalara erişim talepleri e-posta/resmi yazı ile ağ yöneticisine iletilmelidir.
- Daha fazla güvenlik gerektiren sistemler otonom bir ağda tutulmalı ve bağımsız güvenlik sistemlerine sahip olmalıdır.
- Tüm ağ bileşenlerinin konfigürasyonu tanımlanmalı ve uygun filtreleme programları kullanılmalıdır.
- Kurum içi ağlar, Kurumun güvenli bölgelerine göre bölünmelidir.
- İnternet erişimi olan server'lar güvenlik duvarı ile korunmalıdır.
- Sadece Kurum tarafından yetkilendirilmiş bilgisayarların, birim içi ağa giriş izni olmalıdır.
- Sadece işini yapabilmesi için internet erişimine ihtiyaç duyan çalışanların internet erişimi bulunmalıdır.
- Personelin sadece işlerine ilişkin internet uygulamalarını kullanmakta olduklarından emin olabilmek için çeşitli sistem kontrolleri kurulmalıdır.
- Networke bağlı bir iş istasyonu, sadece bilgi güvenliği yöneticilerinin belirlediği gerekliliklerin karşılanması durumunda dış ağlarla iletişim kurabilmelidir.
- Bir uzak ortamdaki kurum ağına bağlanılmak istendiğinde birden fazla onay yöntemi kullanılmalıdır. Böylece güvenlik seviyesi artırılmış olur.
- Kurum ağına bağlı iş istasyonlarına erişim, kullanıcı adı ve parolanın girilmesi ile kontrol altına alınmalıdır.
- Bir sistem yöneticisine uzaktan bağlanabilmek için tek bir kullanım parolası gerekir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	40 / 69

- Güvenlik riski oluşturabilecek kritik portlara erişebilmek için onay gereklidir.
- Ziyaretçilerin yanlarında getirdikleri taşınabilir sistemler, kurum ağı ile hiç bir ilişkisi olmayan bir alt ağ aracılığı ile internete bağlanabilmelidir.
- Eşler arası (Peer to Peer) kablosuz ağ erişimine olanak sağlayan yöntemler (ad hoc yöntemi vb.) engellenmelidir.
- Sadece onaylı donanımların kurum ağına bağlanabilmesi için, 802.1x standardı veya NAC çözümleri kullanılarak kurum ağına bağlanan cihazlara kimlik denetimi yapılmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	41 / 69

12.11. Bilgi ve Yazılım Alışveriş Politikası

- Kurumun elektronik transferlere yönelik muhasebe kayıtlarının tutulmakta olduğundan emin olmalıdır. Böylece kurum kayıtları güncel olacaktır.
- Kurum yazılımlarını veya verilerini kullanmakta olan üçüncü taraflar, gerekli koruma ölçütlerini içeren bir yazılı sözleşme imzalamalıdır. Böylece üçüncü tarafların söz konusu bilgiyi izinsiz kullanması, değiştirmesi veya çoğaltması engellenmiş olacaktır.
- Elektronik ortamda sözleşmenin yapıldığı üçüncü taraflarla, kâğıt üzerinde de anlaşma yapılmalıdır. Yazılı sözleşmeler en güvenli sözleşme biçimidir.
- Bilgi ve veri alışverişinden önce dış tarafların kimliklerinin tespit edilmesi gerekir.
- Üçüncü tarafa açılan tüm gizli bilgilerin kesinlikle şifrenmesi gerekir.
- Üçüncü taraflara yollanan bilgisayar ortamı yeni olmalı veya herhangi bir bilgi içermemelidir.
- Kurumun sahasında kullanılan şifreleme yöntemleri ve güvenlik sertifikaları standarda uyum sağlamalı ve finansal kurumların gerekliliklerini karşılamalıdır.
- İş iletişiminin sağlanması için sadece Kurum tarafından yetkilendirilen personelin e-posta adresleri kullanılmalıdır.
- Tüm ödeme bilgileri, bilgisayar sistemine kayıt edilmeden önce şifrenmelidir.
- E-posta ile gönderilen her türlü hassas bilgi şifrenmelidir.
- Gizli bilgiler sadece uygun sunucularda kayıt altına alınmalıdır.
- Yazılım yükleme veya yazılım güncellemelerini yapma ve sistem bakımını gerçekleştirme yetkisi sadece sistem yöneticilerindir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	BGYS-PL01
Yayın Tarihi	06.07.2015
Revizyon Tarihi	04.05.2026
Revizyon No	07
Sayfa No	42 / 69

- Kritik bir dosyada çeşitli değişikliklerin yapılması durumunda, dosyanın en az iki yedeği alınmalıdır.
- Kurum bir e-postanın içeriğinde herhangi bir değişiklik yapılmasını yasaklamalıdır.
- Kurum bilgi sistemleri aracılığı ile gönderilen mesajlar, saldırgan veya ayrımcılık içeren bildirimler içermemelidir. Kurumun bilgi sistemi sadece iş gereklilikleri için kullanılmalıdır.
- Bir e-postaya gizlilik içermekte olduğuna dair bir not eklendiğinde, bu mesajı sadece e-posta gönderilen kişinin maili aldığından emin olunmalıdır.
- E-posta yoluyla gönderilen bilgiler, bu bilginin kimden gelmekte olduğunu, belirli bir geri dönüş adresi içermelidir.
- Faks yoluyla gönderilen gizlilik içeren herhangi bir bilginin şifrelenmiş ve bir kapak sayfası ile kapatılmış olması gerekir. Bunlara ek olarak, alıcıların kendilerine bir faks gönderilmiş olduğu hakkında bilgilendirilmiş olması gerekir.
- Kurum, bilgi sistemi vasıtasıyla gönderilmiş herhangi bir bilgiyi algılayabilmeli veya zararlı olabileceğini düşündüğü herhangi bir veriyi silme hakkında sahip olmalıdır.
- Personel gizlilik içeren bilgileri sesli mesajlaşma sistemlerine kayıt etmemelidir.
- Toplantılarda yapılan video konferanslar, yönetim veya katılımcılar tarafından izin verilmedikçe kayıt edilmemelidir.
- İşle ilgili tüm aramalar Kurum telefonları ile yapılmalıdır.
- Gizlilik içeren bilgilerin umumi yerlerde konuşulmaması gerekir.
- Kuruma ait kredi kartı numaraları varsa, bu numaralar sadece Kurum telefonu kullanıldığında, telefon aracılığı ile iletilebilir.
- Posta aracılığı ile gönderilen gizli bilgiler iki zarf içinde yollanmalıdır. Dış zarfta, içerideki bilginin hassaslığı ile ilgili hiç bir bilgi yazmamalı, ancak iç zarfta bilginin gizli olduğu belirtilmelidir.
- Kâğıt üzerindeki gizli bilgilerin gönderilmesi durumunda, bilgilerin taahhütlü yollanması gerekir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı

Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	43 / 69

- İç dokümanlardaki herhangi bir değişiklik talebi, değişikliği talep eden kişinin kim olduğunu göstermelidir.
- Kablosuz bağlantı ile gönderilen bilgilerin yollanmadan önce şifrenmesi gerekir.
- Gizli bilgilerin bir toplantıda tartışılması durumunda, toplantı süresince, bu bilginin gizli olduğu ve dinleyenlerin bu bilginin gizliliğini korumaları gerektiği belirtilmelidir.
- Kurumun intranetine yerleştirilen her bilgi veya uygulama daha önceden yetkili kişiler tarafından onaylanmalı ve Kuruma ait olarak kalmaya devam etmelidir. Bu bilgiler Kurum bilgileri olarak saklı tutulmalıdır.


Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	44 / 69

12.12. Bilgi Koruma Politikası

- Her bilgi için verinin sahibi tanımlanmalıdır. Veri Sahibi, o bilgiyi hazırlayan ve üreten birimdir.
- Veri sahibi; elektronik ortamdaki verileri için, her bir çalışanına, verinin hassasiyeti, önemi, güvenlik ve izleme ihtiyaçları konusunda bilgi vermelidir.
- Veri sahibinin izni olmadan; birim personeli, sahibi olmadığı elektronik ortamdaki veri üzerinde herhangi bir aksiyon ve işlem gerçekleştiremez.
- Sunucularındaki kritik verilerin yedeklenmesi, geri yüklenmesi, güvenli bir ortamda muhafaza edilmesi, veri sahibi tarafından öngörülen bilgi erişim hakları için gerekli kontrol ve önlemlerinin alınmasından Bilgi İşlem Dairesi Başkanlığı sorumludur.
- Kritik sunuculardaki veri ve yazılımların Kurum dışı mahallere yedeklenmesi gerçekleştirilmelidir.
- Hiçbir personel yasa dışı ve yasak yazılımı Kurum içinde kullanamaz.
- Yazılım satın alma yetkisi Bilgi İşlem Dairesi Başkanlığı'na aittir. Satın alınan herhangi bir yazılım; Başkanlık tarafından test edilmeden ve kullanıcının yöneticisinin izni olmadan bilgisayarlara yüklenemez. Güvenlik ihlaline sebep olduğu anlaşılan izinsiz programın sorumluluğu kullanıcıya aittir, bu konudaki yaptırımlar kullanıcıya uygulanır.
- Gerçek ortama taşınmadan önce tüm uygulama ve sistem yazılımları test ortamlarında teste tabi tutulmalıdır.
- Tüm personel, kendilerine tahsis edilen yetki çerçevesinde bilgilere erişim sağlamalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	45 / 69

- Herkese açık bir sistemde kullanılabilir yapılmış bilginin bütünlüğü, yetkisiz değiştirmeyi önlemek için korunmalıdır.

12.13. Sunucu Güvenliği Politikası

- Sunucular, fiziksel olarak güvenli ortamlarda tutulmalıdır. Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve kayıt altına alınmalıdır.
- İstemci ve sunucu uygulamalarında dosyalarda ve çerezlerde geçici olarak tutulan kişisel verilerin işleme gereksinimi veya kanuni saklama süresi sona erdiğinde güvenlik ihlali oluşturmayacak şekilde (geri getirilemeyecek, tekrar elde edilemeyecek vb.) yok edilmelidir.
- Sunucuların normal işleyişi için gerekli olmayan tüm servisler kapatılmalıdır. Sistemlerde çalışan servisler ihtiyaçları olan en az yetki ile çalışmalıdır. Servis kullanıcılarının yetkileri ayrıca kısıtlanmalıdır. Servislerin döndüğü başlık bilgileri (banner) bilgi ifşasına yol açmayacak şekilde değiştirilmelidir.
- Güncel ve güvenlik desteği devam eden işletim sistemleri kullanılmalıdır. Uygulama sürümleri periyodik olarak kontrol edilmelidir.
- Tüm sunucularda kullanılmayan kablosuz ağ ara yüzleri pasif hale getirilmelidir.
- Sunucularda ilgili NTP ayarlamaları yapılarak tüm sunucularda zaman senkronizasyonu sağlanmalıdır.
- İşletim sistemi güncellemeleri için merkezi bir güncelleme sunucusu oluşturulmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	46 / 69

- Tüm sunucu ve makinelerde iz kayıtları aktif edilmelidir. Sistem zaman ve tarih ayarları, kullanıcı hesapları, ağ yapılandırması, erişim kontrolleri üzerinde yapılan değişiklikler kayıt altına alınmalıdır. Ayrıca giriş ve çıkış bilgileri, yetkisiz dosya okuma denemeleri, dosya silme işlemleri ve sistem yöneticisi hareketleri de kayıt altına alınmalıdır.
- Sunucu ve sistem güvenliğini sağlayabilmek için lisanslı yazılımlar kullanılmalıdır. Kurumun yazılım lisans varlıklarının sayısı, bu lisansların hangilerinin aktif kullanıldığı, kullanılmayan lisansların bilgisinin tutulması gibi ayrıntıları içeren listeleme ile aktif lisans yönetimi yapılmalıdır.
- Web sunucu yazılımı yönetici hesabıyla değil, bu amaç için özel olarak oluşturulmuş bir hesap ile çalıştırılmalıdır. Web sunucusunda bulunan varsayılan hesaplar/parolalar kullanım dışı bırakılmalıdır.
- Sistem odası güvenliğinin sağlanması amacıyla gerekli olan tüm tedbirler alınmalıdır. İş sürekliliği kapsamında ortam izleme yazılımı ile takip edilmelidir.
- Sunuculara ait tüm konfigürasyon bilgileri belgelenmiş ve bu bilgiler Kurum tarafından onaylanmış olmalıdır.
- Her sunucunun, konfigürasyon, işletim sistemi versiyonu, yüklü yama listesi, yedekleme ve geri yükleme prosedürleri belgelenmiş ve güncel olmalıdır.
- Sunuculara, kullanım amacına yönelik olarak işletim sistemi ve diğer yazılımlar kurulmalıdır. Gereksiz yazılım ya da bileşenleri kaldırılmalıdır.
- Sunucu üzerinde çalışan işletim sistemlerinin, sistem yazılımlarının ve güvenlik amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Mümkünse, yama ve anti virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.
- Kurumsal Değişiklik Yönetim Prosedürü, sunucular için de uygulanmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	47 / 69

- Kritik ve önemli sunucular için aynı özellikte yedekleri tutulmalı, bir acil durum yaşanması durumunda bu yedek sunucu hemen devreye alınmalıdır. Mümkünse yedek sunucu, asıl sunucunun devre dışı kaldığını otomatik olarak anlayarak anında onun yerine geçebilmelidir.
- Sunucu günlükleri düzenli aralıklarla denetim ve izlemeye tabi tutulmalıdır.
- Üzerinde çalıştığı uygulamaların başarısı kanıtlandıktan sonra, tüm sunucu güvenlik yamaları yüklenmelidir.
- Sunucuların uzaktan yönetimi gerekiyor ise; yönetim konsolu ve sunucu arasındaki haberleşme, güvenli kanal ve tekniklerle gerçekleştirilmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	48 / 69

12.14. Parola Koruma Politikası

- Parola en az 8 karakter, en az bir sayı, en az bir büyük harf, en az bir karakter(*,!,.,% vb.) içermelidir. Ardışık parolalar (abc123, 12345a vs) ve Türkçe karakterler kullanılmamalıdır.
- Tüm parola alanlarında kullanıcı giriş yaparken kullanıcının parolası varsayılan olarak maskelenmeli ve açık olarak görünmemelidir.
- Unutulan parola işlevi ve diğer kurtarma yolları geçerli parolayı açığa çıkarmamalı ve yeni parola kullanıcıya açık metin olarak gönderilmemelidir.
- Veri tabanlarında varsayılan kullanıcı hesapları ve parolalar kullanılmamalıdır. Veri tabanı kullanıcıları için güçlü parola politikaları oluşturulmalı ve uygulanmalıdır.
- Herhangi bir parola, “Çok Gizli” bilgi olarak muhafaza altına alınmalı ve iş arkadaşı veya başka bir kişiyle paylaşılmamalıdır.
- Bilgisayar sistemlerine ve tüm şifre gerektiren uygulamalara boş parola ile erişmek mümkün olmamalıdır.
- Hiç bir kullanıcı, adını ve kullanıcı ile ilgili bir bilgiyi (doğum tarihi, telefon numarası, anne adı vs) parola olarak kullanmamalıdır.
- Herhangi bir parola bilgisayar sistem dosyalarında düz metin olarak tutulmamalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	49 / 69

- Tüm varsayılan parolalar, sistem kullanılmaya başlamadan önce kullanıcı ve/ya sistem/ağ yöneticileri tarafından verilecektir. Bilgisayarlara ilk tanımı yapılan kullanıcı için; kullanıcı ilk sisteme giriş yaptığında parolasını değiştirmesi sağlanacaktır.
- Kullanıcıya bildirilecek parolalar güvenli bir ortamda iletilmelidir.
- Parolalar telefon veya uzak iletişim ortamlarından herhangi bir kişiye söylenmemelidir.
- Parolalar hatırlanmak maksadı ile kâğıt ortamına yazılmamalı ve görülecek mekânlara ve açık bir şekilde masalara, monitör üstlerine konulmamalıdır.
- Parolalar belli aralıkla değiştirilmek zorundadır. Sistem tarafından 60 günde bir parola değişimi zorlanmaktadır.
- Parolaların unutulması durumunda ilgili Sistem Yöneticisine başvurulmalıdır.
- Parola geçmişi tutulmalı ve hatalı giriş sayısına göre kullanıcı hesapları kilitlemelidir.
- Yetkili hesapların parola özetlerinin çalınması engellenmelidir.
- Etki alanı yöneticisi (domain admin) hesabıyla kullanıcı bilgisayarlarında gerekli olmadıkça işlem yapılmamalı, işlem yapıldığı durumlarda kullanıcı bilgisayarlarının yeniden başlatılması sağlanmalıdır.
- Etkin olmayan oturumlar 15 dakikalık hareketsizlik süresinden sonra kapatılmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	50 / 69

12.15. Uzaktan Bağlantı Politikası

- Kurum ağına uzaktan erişim sadece iş amacı için kullanılmalıdır.
- Uzak ağ bağlantısında kurumun iç ağına uygulanan güvenlik politikaları geçerli olmalıdır.
- Uzak bağlantılar, güçlü kimlik denetimi ile gerçekleştirilmelidir.
- Uzak bağlantılarda yapılan tüm dosya yüklemelerinde antivirüs taramasından geçirilmelidir.
- Veri tabanı sunucularına olan uzak bağlantı, mümkün olduğunca sınırlandırılarak yalnızca yetkili kullanıcıların ve/veya uygulamaların uzaktan erişimine olanak sağlayacak şekilde yapılandırılmalıdır. Bu kapsamda, ilgili sunucularda mevcut yapılandırmalar düzenlenmeli ve ağ katmanında gerekli önlemler alınmalıdır.
- Uzak erişim için yapılan bağlantıda boşa kalma süresi (herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre sınırlanır. Bu süre 1 (bir) saati geçmemelidir.
- Bağlantı yapan kullanıcının hedef bilgisayardaki oturum açma, oturum kapatma gibi kullanıcı hareketleri kayıt altına alınmalı ve söz konusu iz kayıtları en az 1 (bir) yıl süre ile saklanmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	51 / 69

- Uzak çalışma kapsamında uzak masaüstü bağlantısı yapılacaksa, şahısların kendilerine ait kişisel cihazlar veya sahibi bilinmeyen/herkes tarafından erişilebilen terminaller kullanılmamalıdır. Kullanıcıların bu tip terminaller üzerinden uzak masaüstü bağlantısı yaptıklarının tespit edilmesi halinde gerekli yasal ve idari yaptırımlar uygulanır.
- Sunucuya internet üzerinden erişime ihtiyaç olduğu durumlarda VPN üzerinden erişim sağlanmalıdır. MMS protokolünde kimlik doğrulama özelliği aktif bir şekilde kullanılmalıdır.
- Uzak bağlantı yapabilmek için FRM26 VPN Talep Formu doldurulup ıslak imzalı olarak Bilgi Güvenliği ve Kalite Şubesine teslim edilmelidir. PR36 Kimlik Doğrulama ve Yetkilendirme Prosedüründe uzak bağlantı yetkilendirilmesi detaylandırılmıştır.

12.16. Yazılım Geliştirme Politikası

- Sistem geliştirmede, ihtiyaç analizi fizibilite çalışması, tasarım, geliştirme, test ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.
- Uygulamaların kayıt altına aldığı veya kullandığı her türlü bilginin yetkisiz erişime kapalı olması gerekmektedir.
- Veri tabanı, uygulama sunucusu ve web sunucusu gibi kullanılan yazılımların güvenlik yamaları en üst seviyede olmalıdır.
- GET ve POST isteklerindeki HTTP parametreleri değiştirilerek üçüncü şahısların bilgilerine yetkisiz olarak erişilmemelidir.
- Veri tabanı kullanıcısının sadece uygulamanın kullandığı veri tabanı kaynaklarına erişim hakkı olmalıdır.
- Kısıtlı erişim gerektiren bütün URL'lere, servislere, uygulama verilerine, kullanıcı bilgilerine, güvenlik yapılandırma dosyalarına erişim denetlenmelidir.
- Erişime açılan her kaynak kimlik denetimine tabi tutulma yöntemini de kullanmak zorundadır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	BGYS-PL01
Yayın Tarihi	06.07.2015
Revizyon Tarihi	04.05.2026
Revizyon No	07
Sayfa No	52 / 69

- Kurum dışına servislerle veri aktarımı yapılması durumlarında standart güvenlik prensiplerine uygun çalışılmalıdır.
- Güvenli yazılım geliştirme süreçleri ve olgunluk modellerinden faydalanılarak kurumsal yazılım geliştirme süreçleri güncellenmeli ve güvenli yazılım geliştirme yaşam döngüsü uygulanmalıdır.
- Devreye alınan veya güncellenen uygulamalarda sızma testleri ve uygulama güvenliği testleri yapılmalıdır. Tedarik edilen uygulamalar üzerinde sızma testleri gerçekleştirilmelidir. Kurumun kaynak koduna sahip olduğu tüm uygulamalar devreye alım öncesinde kaynak kod analizinden geçirilmelidir.
- Halka açık ağlar üzerinden geçen uygulama hizmetlerindeki bilgi; hileli faaliyetlerden, sözleşme ihtilafından ve yetkisiz ifşadan ve değiştirmeden korunmalıdır.
- Uygulamalar kullanıcı hesaplarının yönetimini sağlayan ara yüzlere sahip olmalı ve bu ara yüzlere yalnızca yetkili kullanıcıların erişebilmesi sağlanmalıdır. Kullanıcı hesapları, geçici (belirli bir süre, koşul vb. boyunca) veya kalıcı (aksi belirtilmedikçe sürekli) olarak kilitlenebilmelidir. Kalıcı olarak kilitlenen hesap üzerindeki geçici kilit kaldırılrsa dahi kilitli kalmalıdır.
- Kullanıcı tanımlamaları, yapılan işlemlerin izlenebilirliğini sağlayacak ve tekil olarak kişi veya sistemi işaret edecek şekilde yapılmalıdır.
- Kaynak kodda veya kaynak kod depolarında gizli bilgiler, API anahtarları ve parolalar yer almamalıdır. Kullanılan tüm kimlik doğrulama bilgileri şifrelenmeli ve korunan bir yerde depolanmalıdır. Açık anahtar altyapısı tabanlı kimlik doğrulama kullanılıyorsa özel anahtara sadece yetkili kullanıcının erişimine izin verecek mekanizmalar mevcut olmalıdır.
- Uygulamanın sahip olduğu sistem ve yapılandırma dosyaları ile denetim kayıtları ve iz kayıtları gibi bilgiler kullanıcı verisiyle aynı konumda (dizin, sistem bölümü vb.) depolanmamalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı

Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**


BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	BGYS-PL01
Yayın Tarihi	06.07.2015
Revizyon Tarihi	04.05.2026
Revizyon No	07
Sayfa No	53 / 69

- Uygulama çok katmanlı mimari (multitier architecture) kullanılarak tasarlanmalı ve her katman için güvenlik mekanizmaları oluşturulmalıdır. Uygulamanın kullandığı veri tabanları ve kayıtlar, internette doğrudan erişilemeyecek şekilde yapılandırılmalıdır. İnternete açık olarak çalışan sunucular (uygulama sunucusu, web sunucu, e-posta sunucuları vb.) DMZ (DeMilitarized Zone) gibi ayrı bir bölgede tutulmalıdır.
- Uygulama, tanımlanan güvenlik olaylarının/işlemlerinin (yetki değişiklikleri, kullanıcı değişiklikleri, kimlik doğrulama işlemleri) başarılı ve başarısızlık durumları için iz kayıtları oluşturabilmelidir. Kayıtların doğruluğunu sağlamak ve bütünlüğünün bozulmasını (log forging) engellemek için iz kayıtları oluşturulurken kullanılan girdiler üzerinde girdi denetimi yapılmalıdır.
- Uygulamanın girdi olarak kullandığı kişisel veri üzerinde girdi/çıkıktı doğrulama eksikliğinden kaynaklı zafiyetlere karşı güvenlik kontrolleri uygulanmalıdır.
- İlgili kişinin açık rızası olmadan kişisel veri web sayfalarının gizli alanlarında saklanmamalıdır. Kişisel veri, tarayıcı ön belleğinde (cache) saklanmamalıdır. Uygulamada kullanılan çerezlerin kişisel veri içermesi zorunluluk ise secure bayrağı (secure flag) kullanılmalıdır. Ayrıca, istemci tarafında web depolama (web storage) özelliği ile kişisel veriler kayıt altına alınmamalıdır.
- Kişisel veri üzerinde işlem yapılması ana amaç olmayan durumlarda (Adres bilgileri güncellenirken T.C. kimlik numarasının maskelenmesi, hesap numarasına havale işleminde alıcının adının maskelenmesi vb.) uygulama kişisel veriyi maskeleyerek göstermelidir.
- Kişisel verinin yetkisiz bir şekilde değiştirilmesini engellemek için uygun kriptografik yöntemler uygulanmalıdır.
- Özel nitelikli kişisel verinin işlenmesi ve kişisel verinin üçüncü kişilere aktarılması durumunda açık rıza uygulama üzerinden alınmalı ve açık rıza beyan durumu sorgulanabilmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı

Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	54 / 69

- Uygulama üzerinde açık rıza metni yetkili kişiler tarafından güncellenebilmelidir. Güncelleme öncesindeki açık rıza metinleri saklanmalıdır. Güncellenen açık rıza metinleri için kullanıcılardan tekrar açık rıza alınması sağlanmalıdır.

12.17. Erişim Kontrol Politikası

- Bilgi güvenliğini sağlamanın en temel yolu, bilgi varlığına yetkisiz kişilerin erişimlerini engellemek ve yetkisi olan kişilerin erişimlerini de ihtiyaca göre kısıtlamaktır. Her bir erişim için mutlaka Kurum tarafından belirlenmiş erişim yetkilendirme yöntemleri kullanılmalıdır. Erişimlerin takibi ve kontrolü Aktif Dizin(Active Directory) ile yapılır, altı ayda bir kontrol edilir. FRM46 Erişim Kontrol Formu üzerinde kayıt yapılır ve her yıl sonunda bu form Bilgi Güvenliği ve Kalite Şubesine teslim edilmelidir.
- Yetki erişim talepleri BİDB Servis üzerinden gerçekleşmektedir. Talepler ilgili birim sorumlusuna sistem üzerinden ulaştırılarak onayı alınır. Kritik yetkilendirmeler resmi yazı ile gerçekleştirilmelidir.
- Erişim kontrolleri yapılırken GT05 Görev Tanımları dikkate alınır. Kullanıcı kimlik bilgileri ve gizli kimlik doğrulama bilgileri kullanımı, kullanıcı erişim haklarının verilmesi ve kaldırılması, ayrıcalıklı erişim rollerinin kullanımı bu doküman ile açıklanmaktadır.
- Ağa bağlanacak bilgisayarların ağ yöneticileri tarafından belirlenecek ölçütleri taşıyan, kimliği tanımlanmış ve doğrulanmış olması gerekir. Bu maksatla mümkünse ağ tabanlı erişim kontrol sistemleri (NAC) kullanılmalıdır. NAC tabanlı çözümlerin olmaması

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

BİLGİ GÜVENLİĞİ POLİTİKASI


Doküman No	BGYS-PL01
Yayın Tarihi	06.07.2015
Revizyon Tarihi	04.05.2026
Revizyon No	07
Sayfa No	55 / 69

durumunda, ağa bağlanacak cihazların MAC adresleri, bağlanacağı kenar anahtarın ilgili portuna elle tanımlanarak yetkisiz, kimliği bilinmeyen cihazların ağa erişimi engellenmelidir.

- Bilgiye kimin hangi yetki ile erişeceği kararı, bizzat bilgi varlıklarının sahipleri tarafından verilmelidir. Erişim hakları periyodik olarak incelenmelidir.
- Bilgi varlıklarına yapılan erişimler için iz kayıtları tutulmalıdır.
- Bireysel kullanıcı erişim hakları, terfi veya sorumlulukların değiştirilmesi veya görev yeri değişiklikleri sonrasında gözden geçirilmelidir.
- Sunucu ve hizmetlere parolasız erişim engellenmelidir.
- Sistemlere erişimlerde ortak hesap kullanılmamalıdır.
- Sistemlere yapılan tüm erişimlerin olay kayıtları tutulmalı, bozulmaya karşı korunmalı ve ilgili mevzuatta belirtilen sürelerce saklanmalıdır.
- Sistem yöneticisi rolündeki personel, sunucu ve hizmetler üzerinde her türlü işlem için tam yetkilendirilmelidir.
- Sistem, ağ ve kaynaklarına erişim kontrolünde güvenli kimlik doğrulama yöntemleri kullanılmalıdır.
- Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılmalı VTYS sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenmelidir.
- PR36 Kimlik Doğrulama ve Yetkilendirme Prosedüründe erişim süreci detaylandırılmıştır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı


Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	56 / 69

12.18. Kimlik Doğrulama ve Yetkilendirme Politikası

- Kurum sistemlerine erişecek tüm kullanıcıların hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği Aktif Dizin ile belirlenmektedir.
- Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri, ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, denetim altında tutulmalıdır.
- Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.
- Kullanıcılar da Kurum tarafından kullanımlarına tahsis edilen sistemlerin güvenliğinden sorumludur.
- Sistemlere başarılı ve başarısız erişim logları düzenli olarak tutulmalı, tekrarlanan başarısız log-on girişimleri incelenmelidir.
- Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
- Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir. Kullanıcı haklarını izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	57 / 69

- Erişim hakları belirlenen periyotlarda gözden geçirilmeli, Ayrıcalıklı erişim hakları daha sık periyotlarla gözden geçirilmelidir.
- PR36 Kimlik Doğrulama ve Yetkilendirme Prosedüründe süreç detaylandırılmıştır.

12.19. Kriptografik Kontrollerin Kullanımı Politikası

- ‘Gizli’ seviyeli bilgi varlıkları elektronik ortamda şifrelenerek iletilir ve saklanır. Kriptografik kontroller aşağıdaki nedenlerden dolayı kullanılır;
Gizlilik: Saklanan veya iletilen hassas veya kritik bilgiyi korumak için şifrelenerek iletilmesi ya da saklanması.
Bütünlük/Güvenilirlik: Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için elektronik imzaların veya mesaj doğrulama gibi yöntemlerin kullanılması.
İnkâr edilemezlik: İstenmeyen bir olayın, faaliyetin oluştuğunun veya oluşmadığının kanıtlanması gerektiği durumlarda kriptografik tekniklerin kullanılması.
- Veri iletimi ve veri saklanması için kullanılacak şifreleme metotlarının farklı olması gerekmektedir. Metot seçilirken aşağıdaki kriterler göz önünde bulundurulur:
Kullanılabilecek en güncel metotlar tercih edilmelidir. Seçilecek metodun güvenlik açıkları kullanımdan önce araştırılmalıdır. Şifreleme bloğu en az 256 bit olarak seçilmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	58 / 69

- Veri iletişimi esnasında kullanılacak sertifikalar güvenilir kaynaklardan temin edilmeli ya da kurum tarafından üretilmelidir.
- Veri barındıran ve taşıyan sistemlerin kullanacağı şifreleme metotları, işletim sistemi tarafından desteklenen ya da işletim sistemine ait şifreleme yazılımlarından seçilmelidir.
- Şifreleme yönetiminin geri dönüş sağlaması için gerekli anahtarlar farklı ortamda yedeklenmelidir.
- Güvenlik açığı tespit edilmiş anahtarlar kullanılmamalıdır. Anahtarlar kullanımdan kaldırılmadan önce o anahtar ile şifrelenmiş veriler üzerindeki şifreleme kaldırılır ve şifresiz erişim kontrol edilmelidir. Kullanılmayacak anahtarlar tekrar kullanılmayacak şekilde imha edilmelidir.
- Uygulamada şifreleme, anahtar değişimi, dijital imzalama veya özet alma gibi fonksiyonlar bulunuyorsa TS ISO/IEC 19790-24759 onaylı kriptografik modüller ve rastgele sayı üreteçleri kullanılmalıdır.
- Kriptografik kontroller ilgili yasa ve yönetmeliklere uygun olarak belirlenmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi


 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	59 / 69

12.20. Temiz Masa - Temiz Ekran Politikası

Masalarda ya da çalışma ortamlarında korumasız bırakılmış bilgiler yetkisiz kişilerin erişimleriyle gizlilik ilkesinin ihlaline, yangın, sel, deprem gibi felaketlerle bütünlüğünün bozulmalarına ya da yok olmalarına sebep olabilir. Tüm bu veya daha fazla tehditleri yok edebilmek için aşağıda yer alan belli başlı temiz masa kurallarına çalışanlar tarafından uyulması sağlanmalıdır.

- Kullanıcı, başkaları tarafından görülmemesi gereken belgeleri kesinlikle masa üzerinde bulundurmamalıdır. Masa başından ayrılırken, gün içerisinde çalıştığı kritik belgeleri, masa üzerinden mutlaka kaldırılmalıdır. Bu gibi bilgi ve belgeler kilitli dolap, çelik kasa ya da arşiv odası gibi fiziki koruması olan güvenli alanlarda muhafaza edilmelidir.
- Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler güvenli imha yöntemleri ile imha edilmelidir.
- Sistemlerde kullanılan parola, telefon numarası ve T.C. kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulundurulmamalıdır.
- Kullanıcı, bilgisayarını belli bir süre kullanmadığı zaman otomatik olarak şifre ile oturum açmasını gerektirecek şekilde ayarlanmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	60 / 69

- Yetkisiz kişilerin erişiminin engellenmesi için bilgisayar başından ayrılma durumunda ekran kilitlemesi yapılmalıdır.
- Kullanıcı, gizli bilgi içeren evrakı ağ üzerinden paylaşmamalı, gizli bilgi içeren atık evrakı imha etmelidir.
- Kullanıcı, bilgisayarındaki, usb belleğindeki, harici diskindeki ve benzeri veri depolamanın mümkün olduğu ortamlardaki gizlilik dereceli bilgi içeren her türlü belgenin güvenliğini sağlamakla yükümlüdür. Usb veya harici diske gizli/önemli verilerin konulması gerekiyorsa kriptolanarak/şifrelenerek saklanmalıdır.
- Her türlü bilgiler, parolalar, anahtarlar ve bilginin sunulduğu sistemler, sunucular, kişisel bilgisayarlar ve benzeri cihazlar yetkisiz kişilerin erişebileceği bir şekilde parola korumasız ve fiziki olarak güvensiz bir şekilde gözetimsiz bırakılmamalıdır.
- Kurum bünyesinde kullanılan toplantı salonlarında gizli ve kritik bilgi içeren dokümanları toplantı sonrasında ilgili salonlarda bırakmamalı ve salonlardaki tahtalara alınmış notlar silinmelidir.
- Bilgisayar gibi elektronik ortamlarda bulunan bilginin korunması için çalışma saatleri dışında ofis kapıları kilitli tutulmalıdır.
- Faks makinelerine gelen yazılar sürekli kontrol edilmeli ve makinede yazı bırakılmamalıdır.
- Fotokopi ve diğer çoğaltma teknolojilerinin yetkisiz kullanımını önlemek için uygun idari ve teknik tedbirler alınmalıdır.


Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	61 / 69

12.21. Sosyal Medya Kullanım Politikası

- Sosyal medya ve haberleşme uygulamaları arasından yerli uygulamaların kullanımı tercih edilmelidir.
- Kurumsal sosyal medya hesapları üzerinden yapılacak paylaşımlarda kullanılan logo, amblem, sembol, yazı karakteri ile renk uygulamaları Bakanlık standart kullanımına göre gerçekleştirilmelidir.
- Kurumsal hesaplarda, doğruluğu teyit edilmemiş bilgiler paylaşılmamalı, gizlilik esaslarına dikkat edilmelidir.
- Kurumsal hesaplar üzerinden yapılacak paylaşımlarda telif sorunu olmayan ses, müzik, fotoğraf, video gibi her çeşit görsel ve işitsel bilgi, belge, doküman ve materyaller kullanılmalıdır.
- Kurum personeli şahsi hesaplarından paylaşım yaparken, Kurumu temsil ettiğinin bilincinde olmalıdır ve paylaşımlarını bu dikkatle ve özenle yapmalıdır. Kurumu, mesai arkadaşlarını ve idarecileri olumsuz etkileyecek paylaşımlardan kaçınmalıdır.
- Kurum personeli şahsi hesaplarından paylaşım yaparken, siyaset, spor, din ve benzeri toplumsal konularda kişisel ve kurumsal itibarı tehlikeye atacak yorumlar yapmamalı; şikâyet, küfür, kötöleme, aşağılama ve benzeri tutumları içeren paylaşımlar ile tahrik ve tahkir edici söylemlerden kaçınmalıdır.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	62 / 69

- Kurum personeli şahsi hesaplarından paylaşım yaparken, Bakanlığın kurumsal kapasitesi dahilinde işe alım, atama, tayin, görevlendirme gibi personel işlemleri, mal ve hizmet alımı iş ve işlemleri, kamp ve yurt işleri, promosyon ve hediyelik eşyalar gibi her türlü kamusal imkan ile ilgili Kurumu bağlayıcı nitelikte açıklama, taahhüt, vaat veya girişimler ile aldatıcı ve gerçek dışı beyan içeren paylaşımlarda bulunmamalıdır.
- Kurum personeli, şahsi sosyal medya hesapları üzerinden kritik ya da gizlilik değeri olan fiziksel çalışma alanlarına dair herhangi bir bilgiyi-görseli paylaşmamalıdır.
- Kurumsal ve kişisel sosyal medya hesapları kullanılırken, görevin gerektirdiği dikkat ve özen gösterilmeli ve Kuruma ait gizli kalması gereken bilgiler, hiçbir şekilde sosyal medya ortamlarında paylaşılmamalıdır.
- Sosyal medya, alışveriş siteleri, forumlar gibi üyelik isteyen uygulamalarda, Bakanlık tarafından verilen kurumsal e-posta hesapları kullanılmamalıdır. Aksine durumlarda, yapılan tüm işlemlerden ve dile getirilen ifadelerden, ilgili kullanıcı sorumludur.
- Sosyal medya hesaplarına giriş için kullanılan parolalar ile kurum içinde kullanılan parolalar farklı seçilmelidir.
- Eğitimlerde sosyal medya güvenliği ile ilgili hususlara yer verilmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	63 / 69

12.22. Anlık Mesajlaşma Güvenliği Politikası

- Kurumsal haberleşme amacıyla sunucuları kurum kontrolünde olan veya sunucuları yurt içinde bulunan yerli ve milli mesajlaşma uygulamaları kullanılmalıdır. Yerli ve milli olmayan mesajlaşma uygulamalarının kullanıldığı durumlarda oluşabilecek bilgi güvenliği zafiyetleri kullanıcı sorumluluğundadır.
- Uygulamadan gönderilen tüm mesajlar ve uygulama kullanılarak yapılan tüm sesli ve görüntülü aramalar uçtan uca şifrelenmelidir.
- İş amacıyla anlık mesajlaşma uygulamaları üzerinde çalışanlar tarafından oluşturulan grupların açılışında bilgilendirme yapılmalı ve amacına yönelik kullanılmalıdır.
- Bakanlığımız tarafından işlenen kişisel verilerin paylaşılması muhtemel iş ve profesyonel amaçla kurulmuş olan üçüncü kişilerin oluşturduğu gruplarda hiçbir şekilde kişisel veri içeren mesaj ve belgeler paylaşılmamalıdır.


Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	64 / 69

12.23. Mobil Cihaz Kullanım Politikası


- Mobil cihazlar kullanılırken, iş bilgilerinin ele geçirilmemesini temin için özel bir önem gösterilmelidir. Mobil cihaz politikası, korumasız ortamlarda mobil cihazların çalışması riskini hesaba katmalıdır.
- Mobil cihazların kaydı, fiziksel koruma için gereksinimler, yazılım kurulum kısıtlaması, mobil cihaz yazılım sürümleri ve yamaların uygulanması için gereksinimler, bilgi hizmetlerine bağlantı kısıtlaması, erişim kontrolleri, kriptografik teknikler, kötücül yazılım koruması, uzaktan devre dışı bırakma, silme ya da kilitleme, yedekleme, web servislerinin ve web uygulamalarının kullanımı dikkate alınmalıdır.
- Halka açık yerlerde, toplantı odalarında ve diğer korumasız alanlarda mobil cihazların kullanımına dikkat edilmelidir. Bu cihazlar tarafından saklanan ve işlenen bilginin, açıklanmasına ya da yetkisiz erişimine karşı koruma bulunmalıdır.
- Mobil cihazlar; araba ve diğer ulaşım araçları, otel odaları, konferans merkezleri ve toplantı salonları gibi yerlerde hırsızlığa karşı fiziksel olarak da korunmalıdır. Mobil cihazların çalınması ya da kaybolması durumları için yasal, sigorta ve kuruluşun diğer güvenlik gereksinimleri dikkate alınarak özel bir prosedür oluşturulmalıdır.
- Mobil cihaz kullanan personeller için, bu şekilde çalışmalardan kaynaklanan riskler ve uygulanması gereken kontroller ile ilgili olarak farkındalıklarının arttırılması amacıyla eğitim düzenlenmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	65 / 69

- Mobil cihaz politikası kişisel mobil cihazların kullanımına izin veriyorsa, politika ve diğer güvenlik önlemlerinde aşağıdaki hususlara dikkat edilmelidir.
- Cihazların özel ve iş kullanımının ayrılması. Bu ayrımı özel cihazda bulunan iş verisinin ayrılması ve korunması gibi yazılımların kullanılmasını içerir,
- Kullanıcıların görevlerini kabul ettikleri son kullanıcı anlaşmasını imzalamalarından sonra iş bilgilerine erişim sağlanması (fiziksel koruma, yazılım güncelleme vb.), iş verilerinin sahipliğinden feragat, cihazın çalınması ya da kaybolması ya da hizmetin kullanımı yetkilendirmesi için vakit olmadığında kuruluş tarafından verilerin uzaktan silinmesine izin verilmesi. Bu politikada mahremiyet mevzuatının dikkate alınması gerekmektedir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	66 / 69


12.24. Kişisel Veri Saklama ve İmha Politikası

- Kurum tarafından; personel, personel adayları, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, Kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.
- Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5 ve 6 ncı maddelerde ise kişisel verilerin işleme şartları sayılmıştır. Buna göre, Kurumumuz faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.
- Kişisel veri barındıran kayıtlar (resimler, ofis dosyaları vb.) güvensiz ortamlarda (yetkisiz erişim sağlanabilen ortak dizin, harici bellek, disk vb.) saklanmamalıdır.
- İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Kurum tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

1.Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
-------------------	----------

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	67 / 69

Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır.

2. Kişisel Verilerin Silinmesi

- Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
- Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	68 / 69

Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
--	--

3. Kişisel Verilerin Anonim Hale Getirilmesi

- Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, kurum irtibat sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması, geri iadesinin talebi, aktarılması devredilmesi ve elden çıkarılması durumlarında,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	BİLGİ GÜVENLİĞİ POLİTİKASI	Doküman No	BGYS-PL01
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	04.05.2026
		Revizyon No	07
		Sayfa No	69 / 69

- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,
- Kurumun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması durumlarında, Kurum tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, geri verilir veya anonim hale getirilir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi