

|                                                                                                                        |                                        |                                  |                 |
|------------------------------------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------|-----------------|
| <br>GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş. | <b>GÖREVLER AYRILIĞI<br/>PROSEDÜRÜ</b> | Sayfa                            | Sayfa 1 / 6     |
|                                                                                                                        |                                        | Yayın Tarihi                     | 30.12.2025      |
|                                                                                                                        |                                        | Revizyon Tarihi /<br>Revizyon No | -               |
|                                                                                                                        |                                        | Doküman Kodu                     | SNGYO-BT2025-03 |

## 1. AMAÇ

Görevler ayrılığı ile hedeflenenler:

- **Hata ve suistimal riskini azaltmak**  
(Tek kişinin yaptığı hatayı veya kötü niyetli işlemi gizlemesi zorlaşır.)
- **Çıkar çatışmalarını önlemek**  
(Kendi kararını kendi onaylayan, kendi işlemini kendi kontrol eden kişi olmasın.)
- **Daha güçlü iç kontrol ve denetlenebilirlik sağlamak**  
(İşlemler en az iki gözden geçer.)
- **Şeffaflık ve hesap verebilirlik**  
(Kim neyi yaptı, kim neyi onayladı netleşir.)

## 2. TEMEL MANTIK

### İnisiyatif – Onay – Kontrol Ayrılığı

Kritik süreçlerde şu roller mümkün olduğunca farklı kişilerde olmalıdır:

1. **Başlatan (Initiator)**
  - Talebi oluşturan, işi başlatan.
2. **Onaylayan (Approver / Authorizer)**
  - Yapılacak işlemi kontrol edip uygunluğunu onaylayan.
3. **Gerçekleştiren (Executor)**
  - Fiziksel veya sistemsal işlemi fiilen yapan.
4. **Kontrol eden / Raporlayan (Controller)**
  - İşlemleri geriye dönük inceleyen, raporlayan.

Küçük kurumlardaki kısıtlı personel durumunda bile, en azından “yapan” ve “onaylayan” rollerinin ayrılması kritik kabul edilir.

## 3. ÖRNEKLER İLE GÖREVLER AYRILIĞI

### 3.1. Finans / Muhasebe Örneği

#### Uygun olmayan durum:

- Aynı kişi;
  - Cari kart açıyor,
  - Fatura kesiyor,
  - Banka ödeme talimatını oluşturuyor,
  - Ödemeyi onaylıyor.

Bu durumda kişi hem borç yaratıyor hem ödemeyi başlatıyor, hem de kendi işini onaylıyor olur.

#### Uygun Görevler Ayrılığı:

- **Personel A:** Satın alma talebini oluşturur.
- **Personel B (Yönetici):** Satın alma talebini tutar ve onaylar.
- **Personel C (Muhasebe):** Faturayı sisteme işler.
- **Personel D (Finans Yetkilisi):** Ödeme talimatını onaylar ve bankada işlemi gerçekleştirir.
- **Personel E (İç Denetim veya Üst Yönetim):** Dönemsel mutabakat ve kontrol yapar.

|                                |                            |
|--------------------------------|----------------------------|
| <b>HAZIRLAYAN</b>              | <b>ONAYLAYAN</b>           |
| BİLGİ TEKNOLOJİLERİ DEPARTMANI | MALİ İŞLER GRUP BAŞKANLIĞI |

|                                                                                                                        |                                        |                                  |                 |
|------------------------------------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------|-----------------|
| <br>GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş. | <b>GÖREVLER AYRILIĞI<br/>PROSEDÜRÜ</b> | Sayfa                            | Sayfa 2 / 6     |
|                                                                                                                        |                                        | Yayın Tarihi                     | 30.12.2025      |
|                                                                                                                        |                                        | Revizyon Tarihi /<br>Revizyon No | -               |
|                                                                                                                        |                                        | Doküman Kodu                     | SNGYO-BT2025-03 |

### 3.2. Satın Alma Süreci Örneği

- Talep eden birim sadece “ihtiyaç talebini” girer.
- Satın alma birimi teklif toplar, tedarikçi seçimi için dosya hazırlar.
- Yönetici/Komite “tedarikçi seçimi + bütçe onayı” yapar.
- Lojistik/Depo mal kabul ve sayımını yapar.
- Muhasebe faturayı kaydeder.

Burada talep, onay, alım, teslim alma ve muhasebe fonksiyonları ayrıştırılmıştır.

### 3.2. Satın Alma Süreci Örneği

- Talep eden birim sadece “ihtiyaç talebini” girer.
- Satın alma birimi teklif toplar, tedarikçi seçimi için dosya hazırlar.
- Yönetici/Komite “tedarikçi seçimi + bütçe onayı” yapar.
- Lojistik/Depo mal kabul ve sayımını yapar.
- Muhasebe faturayı kaydeder.

Burada talep, onay, alım, teslim alma ve muhasebe fonksiyonları ayrıştırılmıştır.

### 3.3. Bilgi Teknolojileri (IT) Örneği

#### Uygun olmayan durum:

- Aynı BT personeli;
  - Active Directory’de kullanıcı hesaplarını açıyor/siliyor,
  - Kullanıcılara yetkileri tanımlıyor (gruplara üye yapıyor),
  - Logları yönetiyor/siliyor,
  - Sistem yedeklerine erişiyor ve geri dönüşleri kendi başına yapıyor,
  - Canlı sistemlere kod/değişiklik geçiriyor.

Bu durumda kişi hem yetki veriyor, hem işlem yapıyor, hem de kendi yaptığı işlemin izini silebilecek pozisyona geliyor.

#### Uygun Görevler Ayrılığı (örnek model):

- Uygulama Geliştirme (Developer):**
  - Kod geliştirir, test ortamına aktarır.
  - Canlı ortama doğrudan erişimi yoktur.
- Sistem / Uygulama Yöneticisi (SysAdmin/AppAdmin):**
  - Canlı ortamda sürüm geçişini yapar.
  - Kullanıcı hesaplarının teknik işletimini yapar, ancak hangi kullanıcıya hangi yetkinin verileceği iş birimi onayına bağlıdır.
- Yetki Sahibi İş Birimi Yöneticisi (Process Owner):**
  - Hangi kullanıcının hangi yetkiyi alacağını onaylar (Rol bazlı).
- Güvenlik / Denetim (InfoSec / Internal Audit):**
  - Logları takip eder, ayrı bir yetkilendirme ile erişir.
  - Kullanıcı-yetki matrisini ve SoD çatışmalarını kontrol eder.

|                                       |                                   |
|---------------------------------------|-----------------------------------|
| <b>HAZIRLAYAN</b>                     | <b>ONAYLAYAN</b>                  |
| <b>BİLGİ TEKNOLOJİLERİ DEPARTMANI</b> | <b>MALİ İŞLER GRUP BAŞKANLIĞI</b> |

|                                                                                                                        |                                        |                                  |                 |
|------------------------------------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------|-----------------|
| <br>GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş. | <b>GÖREVLER AYRILIĞI<br/>PROSEDÜRÜ</b> | Sayfa                            | Sayfa 3 / 6     |
|                                                                                                                        |                                        | Yayın Tarihi                     | 30.12.2025      |
|                                                                                                                        |                                        | Revizyon Tarihi /<br>Revizyon No | -               |
|                                                                                                                        |                                        | Doküman Kodu                     | SNGYO-BT2025-03 |

**Örnek çatışma (SoD conflict):**

- “Ödeme talimatı oluşturma” ve “ödeme onaylama” yetkilerinin aynı kullanıcıda olması.
- “Sipariş girme” ve “sipariş silme” yetkilerinin aynı kullanıcıda olması.
- “Yeni kullanıcı oluşturma” ve “kullanıcı silen log kayıtlarını silebilme” yetkisinin aynı kullanıcıda olması.

**4. GÖREVLER AYRILIĞI İLKESİ KURUMSAL CÜMLE ÖRNEĞİ**

Kurum bünyesinde yürütülen kritik süreçlerde (finans, satın alma, insan kaynakları, bilgi sistemleri vb.) “işlemi başlatan, işlemi gerçekleştiren, işlemi onaylayan ve işlemi kontrol eden” görevler mümkün olduğunca farklı kişiler tarafından yürütülür. Aynı kişi, bir işlemin hem başlatılması hem sonuçlandırılması hem de kontrolü üzerinde eşzamanlı yetki sahibi olamaz. Personel sayısının sınırlı olduğu durumlarda, asgari olarak “işlemi yapan” ve “işlemi onaylayan” görevleri farklı kişiler tarafından yerine getirilir ve bu durum yazılı olarak gerekecektir.

**5. GÖREVLER AYRILIĞI MATRİS ÖRNEKLERİ**

İki parçadan oluşur;

1. Görevler vs Roller Matrisi (kim neyi yapar/onaylar/denetler)
2. Çatışan Roller Matrisi (aynı kişide olmaması önerilen rol çiftleri)

**5.1 Roller :**

Bu roller satır/sütunlarda kullanılacak;

- R1 – Uygulama Geliştirici (Developer)
- R2 – Uygulama Yöneticisi (App Admin)
- R3 – Sistem / Altyapı Yöneticisi (SysAdmin)
- R4 – Veritabanı Yöneticisi (DBA)
- R5 – Bilgi Güvenliği Uzmanı / Yöneticisi (InfoSec)
- R6 – Yardım Masası / Destek (Helpdesk)
- R7 – İş Birimi Süreç Sahibi (Process Owner / Birim Yön.)
- R8 – İç Denetim / Uyum (Internal Audit / Compliance)

**5.2 Görevler ve Roller Matrisi:**

**5.2.1 Kullanıcı ve Yetki Yönetimi**

|                                       |                                   |
|---------------------------------------|-----------------------------------|
| <b>HAZIRLAYAN</b>                     | <b>ONAYLAYAN</b>                  |
| <b>BİLGİ TEKNOLOJİLERİ DEPARTMANI</b> | <b>MALİ İŞLER GRUP BAŞKANLIĞI</b> |

|                                                                                                                                                            |                                        |                                  |                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------|-----------------|
| <br><b>SİNPAŞ GYO</b><br><small>GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.</small> | <b>GÖREVLER AYRILIĞI<br/>PROSEDÜRÜ</b> | Sayfa                            | Sayfa 4 / 6     |
|                                                                                                                                                            |                                        | Yayın Tarihi                     | 30.12.2025      |
|                                                                                                                                                            |                                        | Revizyon Tarihi /<br>Revizyon No | -               |
|                                                                                                                                                            |                                        | Doküman Kodu                     | SNGYO-BT2025-03 |

| No | Görev                                                                | R1<br>Dev | R2<br>AppAdmin | R3<br>SysAdmin | R4<br>DBA | R5<br>InfoSec | R6<br>Helpdesk | R7<br>Süreç<br>Sahibi | R8<br>İç Denetim |
|----|----------------------------------------------------------------------|-----------|----------------|----------------|-----------|---------------|----------------|-----------------------|------------------|
| 1  | AD / uygulamada kullanıcı hesabı açma/kapatma                        | -         | Y              | Y              | -         | K             | Y*             | O                     | K                |
| 2  | Kullanıcıya rol / yetki atama (fonksiyonel rol)                      | -         | Y              | -              | -         | K             | -              | O                     | K                |
| 3  | Kritik yetki taleplerini onaylama (örn. admin, finans kritik roller) | -         | -              | -              | -         | O/K           | -              | O                     | K                |
| 4  | Yetki matrisi / rol tasarımı (iş + IT birlikte)                      | -         | Y              | -              | -         | K             | -              | O                     | K                |
| 5  | Periyodik yetki gözden geçirme (user-access review)                  | -         | -              | -              | -         | K             | -              | O                     | K                |

\* R6 Helpdesk için; sadece önceden tanımlanmış, düşük riskli standart roller çerçevesinde ve R7 onayı ile.

#### 5.2.2 Uygulama Geliştirme ve Değişiklik Yönetimi

| No | Görev                                                       | R1<br>Dev | R2<br>AppAdmin | R3<br>SysAdmin | R4<br>DBA | R5<br>InfoSec | R6<br>Helpdesk | R7 Süreç<br>Sahibi | R8 İç<br>Denetim |
|----|-------------------------------------------------------------|-----------|----------------|----------------|-----------|---------------|----------------|--------------------|------------------|
| 6  | Uygulama kod geliştirme (dev, test ortamı)                  | Y         | -              | -              | -         | -             | -              | -                  | -                |
| 7  | Kod inceleme / peer review                                  | Y         | -              | -              | -         | K             | -              | -                  | K                |
| 8  | Canlı ortama kod / sürüm geçişini başlatma (change request) | -         | O              | -              | -         | K             | -              | O                  | K                |
| 9  | Canlı ortama kod / sürüm geçişinin uygulanması              | -         | Y              | Y              | -         | K             | -              | -                  | K                |
| 10 | Değişiklik kaydını (change record) kapatma ve dokümantasyon | -         | Y              | Y              | -         | K             | -              | O                  | K                |

**Not:** Geliştiricinin (R1) doğrudan canlı ortama kod geçmemesi Görevler Ayrılığı açısından kritik.

|                                |                            |
|--------------------------------|----------------------------|
| HAZIRLAYAN                     | ONAYLAYAN                  |
| BİLGİ TEKNOLOJİLERİ DEPARTMANI | MALİ İŞLER GRUP BAŞKANLIĞI |

|                                                                                                                                                            |                                        |                                  |                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------|-----------------|
| <br><b>SİNPAŞ GYO</b><br><small>GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.</small> | <b>GÖREVLER AYRILIĞI<br/>PROSEDÜRÜ</b> | Sayfa                            | Sayfa 5 / 6     |
|                                                                                                                                                            |                                        | Yayın Tarihi                     | 30.12.2025      |
|                                                                                                                                                            |                                        | Revizyon Tarihi /<br>Revizyon No | -               |
|                                                                                                                                                            |                                        | Doküman Kodu                     | SNGYO-BT2025-03 |

### 5.2.3 Sistem, Veri tabanı, Yedekleme

| No | Görev                                               | R1<br>Dev | R2<br>AppAdmin | R3<br>SysAdmin | R4<br>DBA | R5<br>InfoSec | R6<br>Helpdesk | R7 Süreç<br>Sahibi | R8 İç<br>Denetim |
|----|-----------------------------------------------------|-----------|----------------|----------------|-----------|---------------|----------------|--------------------|------------------|
| 11 | Sunucu / işletim sistemi kurulumu ve konfigürasyonu | -         | -              | Y              | -         | K             | -              | -                  | K                |
| 12 | Veritabanı kurulumu ve konfigürasyonu               | -         | -              | -              | Y         | K             | -              | -                  | K                |
| 13 | Veri tabanı şeması değişikliklerinin uygulanması    | -         | -              | -              | Y         | K             | -              | O                  | K                |
| 14 | Sistem yedeklerinin alınması (OS, DB, uygulama)     | -         | Y              | Y              | Y         | K             | -              | -                  | K                |
| 15 | Yedekten geri dönüş (restore) işlemi                | -         | O              | Y              | Y         | K             | -              | O                  | K                |

### 5.2.4 Log Yönetimi ve Güvenlik

| No | Görev                                                                                   | R1<br>Dev | R2<br>AppAdmin | R3<br>SysAdmin | R4<br>DBA | R5<br>InfoSec | R6<br>Helpdesk | R7 Süreç<br>Sahibi | R8 İç<br>Denetim |
|----|-----------------------------------------------------------------------------------------|-----------|----------------|----------------|-----------|---------------|----------------|--------------------|------------------|
| 16 | Uygulama loglarını görüntüleme                                                          | -         | Y              | Y              | -         | K             | -              | -                  | K                |
| 17 | Güvenlik loglarına erişim / SIEM üzerinden izleme                                       | -         | -              | Y              | -         | Y             | -              | -                  | K                |
| 18 | Logların manuel silinmesi / değiştirilmesi                                              | -         | -              | -              | -         | -             | -              | -                  | -                |
| 19 | Güvenlik olay analizi ve inceleme                                                       | -         | -              | Y              | -         | Y             | -              | -                  | K                |
| 20 | Güvenlik olayına ilişkin aksiyonların onayı (hesap kapatma, zorunlu şifre değişimi vb.) | -         | -              | O              | -         | O             | -              | O                  | K                |

**Not: 18. satırda manuel log silme için herkes “-”; log silme sadece otomatik rotasyon ve saklama politikası ile olmalı.**

|                                       |                                   |
|---------------------------------------|-----------------------------------|
| <b>HAZIRLAYAN</b>                     | <b>ONAYLAYAN</b>                  |
| <b>BİLGİ TEKNOLOJİLERİ DEPARTMANI</b> | <b>MALİ İŞLER GRUP BAŞKANLIĞI</b> |

|                                                                                                                                                            |                                        |                                  |                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------|-----------------|
| <br><b>SİNPAŞ GYO</b><br><small>GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.</small> | <b>GÖREVLER AYRILIĞI<br/>PROSEDÜRÜ</b> | Sayfa                            | Sayfa 6 / 6     |
|                                                                                                                                                            |                                        | Yayın Tarihi                     | 30.12.2025      |
|                                                                                                                                                            |                                        | Revizyon Tarihi /<br>Revizyon No | -               |
|                                                                                                                                                            |                                        | Doküman Kodu                     | SNGYO-BT2025-03 |

### 5.2.5 Politika, Uyum ve Denetim

| No | Görev                                                         | R1<br>Dev | R2<br>AppAdmin | R3<br>SysAdmin | R4<br>DBA | R5<br>InfoSec | R6<br>Helpdesk | R7 Süreç<br>Sahibi | R8 İç<br>Denetim |
|----|---------------------------------------------------------------|-----------|----------------|----------------|-----------|---------------|----------------|--------------------|------------------|
| 21 | Bilgi güvenliği politika ve prosedürlerini hazırlama          | -         | -              | -              | -         | Y             | -              | O                  | K                |
| 22 | İç kontrol ve uygunluk değerlendirmesi (SoD, erişim, log vs.) | -         | -              | -              | -         | K             | -              | -                  | Y                |
| 23 | Dış / bağımsız denetim koordinasyonu                          | -         | -              | -              | -         | K             | -              | O                  | Y                |

### 6. ÇATIŞAN ROLLER MATRİSİ (Aynı Kişide Olmaması Gereken Roller)

Bu matriste Ç = Çatışmalı / aynı kişide olmaması gereken roller anlamına geliyor. Boş bırakılan kombinasyonlar kritik çatışma olarak değerlendirilmeyebilir (yine de kurum risk iştahına göre gözden geçirilmeli).

|                                | R1<br>Dev | R2<br>AppAdmin | R3<br>SysAdmin | R4<br>DBA | R5<br>InfoSec | R6<br>İç Denetim |
|--------------------------------|-----------|----------------|----------------|-----------|---------------|------------------|
| R1 Uygulama Geliştirici        | -         | Ç              | Ç              | Ç         | Ç             | Ç                |
| R2 Uygulama Yöneticisi         | Ç         | -              | Ç              | Ç         | Ç             | Ç                |
| R3 Sistem / Altyapı Yöneticisi | Ç         | Ç              | -              | Ç         | Ç             | Ç                |
| R4 Veri tabanı Yöneticisi      | Ç         | Ç              | Ç              | -         | Ç             | Ç                |
| R5 Bilgi Güvenliği Uzmanı      | Ç         | Ç              | Ç              | Ç         | -             | Ç                |
| R6 İç Denetim / Uyum           | Ç         | Ç              | Ç              | Ç         | Ç             | -                |

Bu tablo **idealde** olması gereken ayrışmayı gösteriyor.

Küçük kurumlarda bazı "Ç" işaretli roller zorunlu olarak aynı kişide olabilir; bu durumda:

- "Risk analizi yapılmalı,"
- "Üst yönetimce **risk kabul** edilmeli,"
- "Telafi edici kontroller (daha sık denetim, çapraz kontrol, log inceleme vb.) tanımlanmalıdır."

|                                       |                                   |
|---------------------------------------|-----------------------------------|
| <b>HAZIRLAYAN</b>                     | <b>ONAYLAYAN</b>                  |
| <b>BİLGİ TEKNOLOJİLERİ DEPARTMANI</b> | <b>MALİ İŞLER GRUP BAŞKANLIĞI</b> |