**REVİZYON GEÇMİŞİ**

| Revizyon No | Tarih | Açıklama |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| HAZIRLAYAN | ONAYLAYAN | |
|---|---|---|
| EYSS | Genel Müdür Yardımcısı | Genel Müdür |
| | | |


ELEKTRONİK NÜSHADIR
BASILMIŞ HALİ KONTROLSÜZ KOPYADIR

## 1 AMAÇ VE KAPSAM

Bu politikanın amacı; tüm uygulamaların güvenliğinin sağlanması amacıyla tüm yazılım geliştiriciler, veri tabanı ve sistem yöneticileri tarafından uyulması gereken kuralları ve kontrol edilmesi gereken adımları tanımlamak üzere hazırlanmıştır. Bu doküman, "Kapsam Analizi Dokümanı"nda belirtilen birimleri kapsar.

## 2 ROLLER VE SORUMLULUKLAR

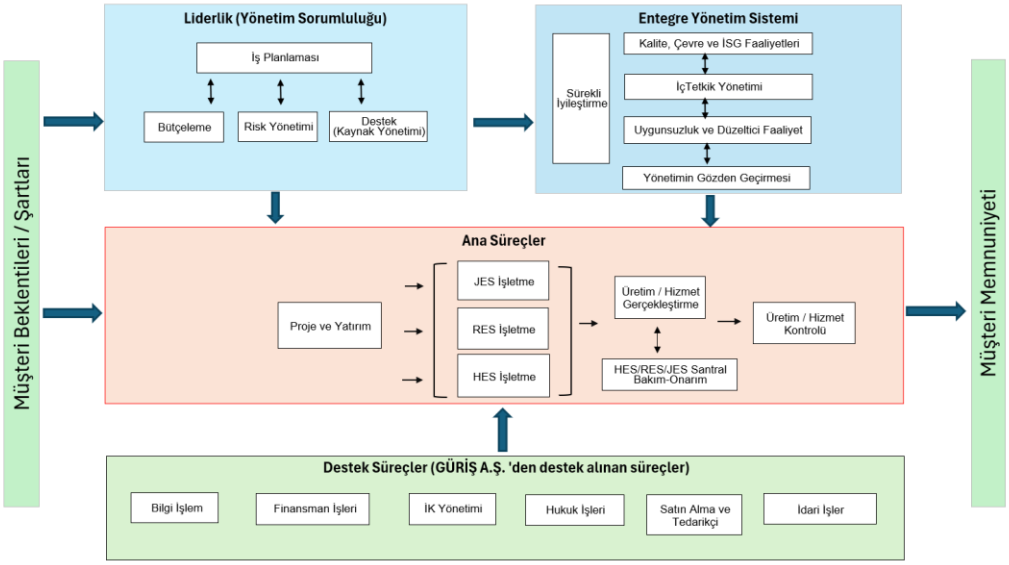
Bu dokümanla ilişkili roller ve sorumluluklar aşağıda listelenmiştir.

| Rol/Unvan / Görev | Üst Yönetim | Üst Yönetim Temsilcisi | BGYS/EYS Yöneticisi | BGYS/EYS Komite Üyeleri | Diğer Çalışanlar |
|---|---|---|---|---|---|
| **Hazırlama** | | | X | X | |
| **Kontrol** | | | X | X | |
| **Onay** | X | X | | | |
| **Yayınlama** | | | X | | |
| **Güncelleme** | | | X | | |
| **Uygulama** | X | X | X | X | X |
| **Uygulamadan Kaldırma** | | X | | | |

## 3 POLİTİKA

Bilgi ve bilgi varlıklarının kullanımı sırasında gizlilik, bütünlük ve erişilebilirliği sağlamak amacıyla tüm bilgi sistemleri ve bilgi teknolojileri süreçlerine ait çalışmalarının gerçekleştirilmesi GÜRİŞ A.Ş. Bilgi İşlem birimi tarafından yönetilmektedir.

**Destek süreçlerine ait, Süreç Etkileşim Haritası**



### 3.1. Veri Koruması

- Uygulamaların kayıt altına aldığı veya kullandığı her türlü bilgi, yetkisiz erişime kapalıdır.
- Uygulama ve veri tabanı sunucularının sistem bileşenleri hakkındaki kritik bilgileri gizlenir.
- Uygulama ve veri tabanı sunucularının güvenlik yamaları en üst seviyededir.
- Uygulama üzerinden yapılan kritik işlemler hem uygulama seviyesinde hem de sunucu seviyesinde kayıt altına alınır.

### 3.2. Erişim Kontrolü

- Uygulamaların yayın yaptığı içerikler, dizinler, sunucuların arayüzleri vb. hiçbir kaynak, kontrol dışı erişilebilir olamaz.
- Veri tabanı kullanıcısının sadece uygulamanın kullandığı veri tabanı kaynaklarına erişim hakkı vardır ve sadece sunucu IP adresinden bağlanır.

### 3.3. Kimlik Sınama

- Erişime açılan her kaynak, kimlik denetimine tabi tutulma yöntemini kullanmak zorundadır.
- Tüm login işlemleri kayıt altına alınır.

### 3.5. Oturum Yönetimi

- Oturum bilgisi zaman aşımına uğrayacak şekilde yapılandırılır.
- Uygulamalarda başarılı kimlik doğrulama ve tekrarlayan kimlik doğrulama (re-authentication) neticesinde her zaman yeni bir oturum bilgisi oluşturulur. Çıkış işleminden sonra da var olan oturum bilgisi geçersizleştirilir.

## 4 İLGİLİ DOKÜMANLAR

### 4.1 Dahili Dokümanlar

- Kapsam Analizi Dokümanı
- Varlık Yönetimi Prosedürü

### 4.2 Harici Dokümanlar

- ISO / IEC 27001:2022 Bilgi Güvenliği, Siber Güvenlik ve Kişisel Gizliliğin Korunması – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler
- ISO / IEC 27019:2020 Bilgi Teknolojisi – Güvenlik Teknikleri – Enerji Hizmet Endüstrisi Bilgi Güvenliği Önlemleri

ELEKTRONİK NÜSHADIR
BASILMIŞ HALİ KONTROLSÜZ KOPYADIR