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; bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunmasıdır. Bu doküman, "Kapsam Analizi Dokümanı"nda belirtilen birimleri kapsar.

2 ROLLER VE SORUMLULUKLAR

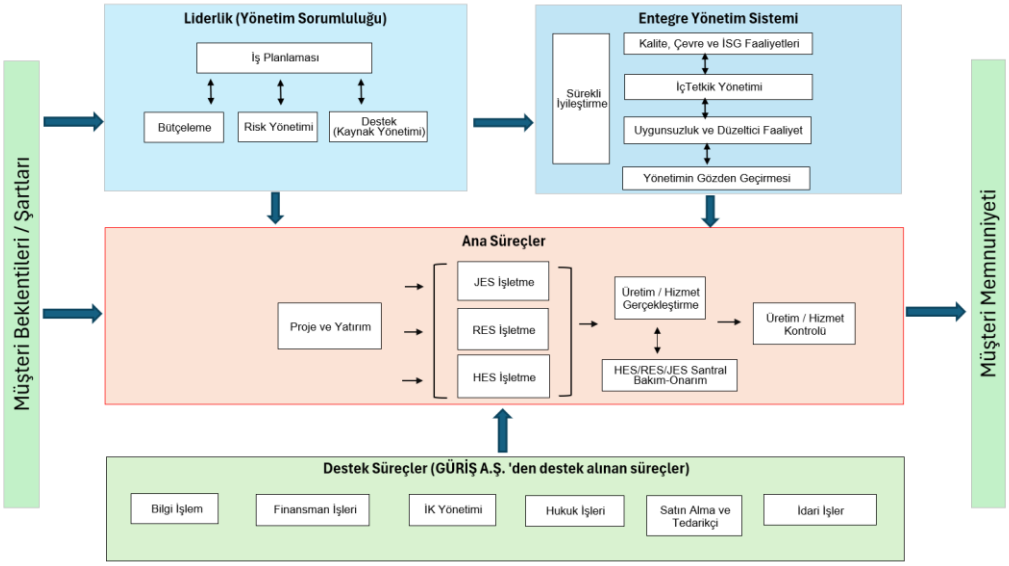
Bu dokümanla ilişkili roller ve sorumluluklar aşağıda listelenmiştir.

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



ELEKTRONİK NÜSHADIR
BASILMIŞ HALİ KONTROLSÜZ KOPYADIR

- Kurum içerisinde tanımlanan gizli bilgi varlıkları kriptografik şifreleme yöntemleri ile saklanır.
- Çalışanlar, kendilerine verilen e-imza, e-fatura, kep vb. kritik bilgi içeren yetki ve kriptografik anahtarların uygun şekilde korumakla sorumludur.
- Risk değerlendirmelerine göre yüksek düzeyde koruma gerektiren bilgi varlıklarının korunmasında güçlü şifreleme algoritması kullanılır.
- Mobil cihazlardaki verilerin korunmasında güçlü şifre yöntemleri kullanılır.
- E-posta hesabı kurulu akıllı telefonlarda telefon kilidi kullanılması zorunludur.
- Tamamlanan şifreler belirli aralıklarla değiştirilir.
- E-posta kurulu tüm sistemlerde Çok Faktörlü Kimlik Doğrulama Yöntemi ile erişim sağlanır.

4 YAPTIRIM VE CEZA

- Bilgi Güvenliği Yönetim Sistemi politika, prosedür ve süreçlerine uyulmaması halinde tanımlanmış disiplin süreçleri kapsamında yaptırım uygulanır.
- Tüm kullanıcılar, kimlik doğrulama bilgilerini korumaktan, bilgi kendi kullanımındayken bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini varlık sahibi tarafından belirlenen önlemlere uygun olarak korumaktan sorumludur.
- Kriptografik Kontroller Politikası tarafından düzenlenen kurallara uymayanlara uygulanacak yaptırım ve cezalar Disiplin Politikası kapsamında değerlendirilir.
- Personel, kurumsal faaliyetleri sırasında elde ettiği ve görüntüleyebildiği kişisel verilerin güvenliğini sağlamakla ve Kişisel Verilerin Korunması Kanunu kapsamında uygun çalışmakla yükümlüdür.

5 İLGİLİ DOKÜMANLAR

5.1 Dahili Dokümanlar

- Kapsam Analizi Dokümanı
- Disiplin Politikası

5.2 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
- 6698 Sayılı Kişisel Verilerin Korunması Kanunu

ELEKTRONİK NÜSHADIR
BASILMIŞ HALİ KONTROLSÜZ KOPYADIR