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, mobil bilgi ve iletişim varlıklarının iş amaçlarına uygun kullanılması amacıyla her tür mobil ve akıllı cihazın yönetimini kurumsal yaklaşımlar çerçevesinde düzenlemeyi amaçlamaktadır. Bilgi varlıklarına erişen ve/veya uzaktan erişim sağlayan, kullanıcılara verilen akıllı telefonları, tabletleri, çalışanların kişisel akıllı telefonlarını, çalışanlar tarafından kullanılan her tür mobil cihazı ve EKS ağındaki akıllı cihazları kapsar. Bu doküman, "Kapsam Analizi Dokümanı"nda belirtilen birimleri kapsar.

2 ROLLER VE SORUMLULUKLAR

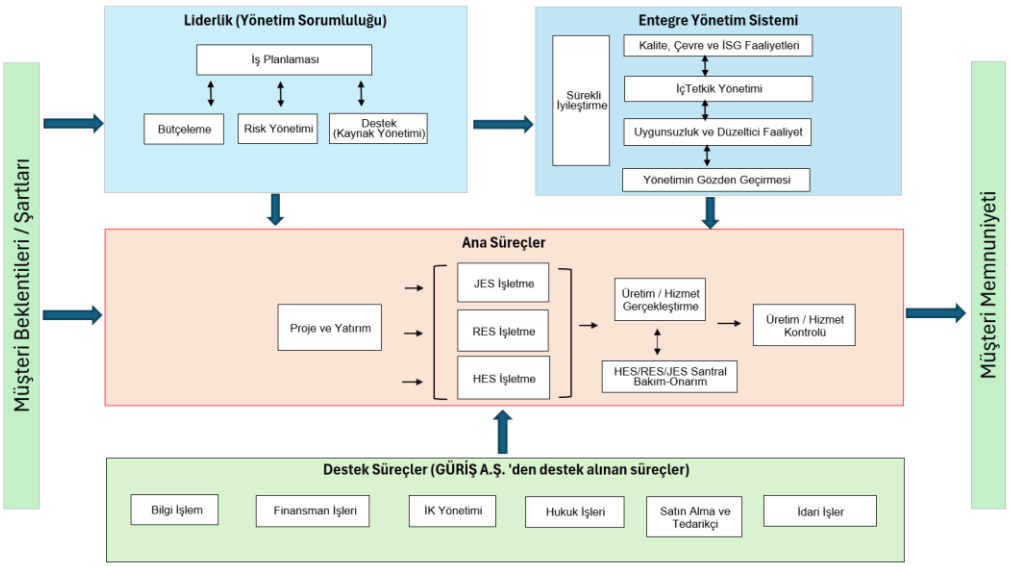
Bu dokümanla ilişkili roller ve sorumluluklar aşağıda listelenmiştir.

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

3.1. Bilgi Sistemleri Mobil Cihaz Güvenliği

- Şirket bilgi kaynaklarına erişmek için, uygunluğu Bilgi İşlem Müdürlüğü tarafından onaylanan mobil cihazlar kullanılır. Taşınabilir mobil cihazlar gözetimsiz bırakıldıklarında mutlaka fiziksel olarak güvenli bir yerde saklanır.
- Şirket çıkarlarıyla çakışmadığı sürece bu cihazların kişisel kullanımına Bilgi İşlem Müdürlüğü tarafından belirlenen kısıtlamalar çerçevesinde izin verilir.
- Şirket ait mobil cihazlar hiçbir şekilde yasa dışı, şirket çıkarlarıyla çelişecek veya normal operasyon ve iş aktivitelerini engelleyecek şekilde kullanılmaz.
- Şirket mobil cihazlar kullanılarak yapılan tüm işlemleri izleme ve kayıt altına alma hakkını saklı tutar. Şirket kullanıcının mobil cihazlar ile gerçekleştirdiği aktivitelerle ilgili bilgiyi, gerekli durumlarda yasal düzenlemeler çerçevesinde kanun uygulayıcılarla paylaşabilir.

3.2. Endüstriyel Akıllı Cihaz Güvenliği

- Akıllı/endüstriyel sayaç yapısında yer alan tüm bileşenlerin ve iletişim cihazlarının bir envanteri oluşturulmuştur.
- Akıllı/endüstriyel sayaç yapısında yer alan tüm bileşenler "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddelerine uygun şekilde periyodik olarak güvenlik testlerine tabi tutulmaktadır.
- Akıllı/endüstriyel sayaç yapısında yer alan tüm bileşenler risk yönetim süreci içerisinde değerlendirilmiştir.
- Akıllı/endüstriyel sayaç yapısında yer alan bileşenlerden alınan logların saklanmasına ilişkin süreler ilgili yasal düzenlemelere uygun olarak belirlenmiştir.
- Akıllı/endüstriyel sayaç yapısında kullanılan bileşenler üzerinde tutulan, işlenen ve saklanan tüm veriler için ilgili yasal düzenlemelere uygun hareket edilmektedir.
- Akıllı/endüstriyel sayaç yapısında kullanılan bileşenler üzerinde çalışan servisler belirlenmiş ve gereksiz olduğu değerlendirilen servisler devre dışı bırakılmıştır.
- Akıllı/endüstriyel sayaç yapısına ilişkin risk analizi sürecinde tüm mimariye ilişkin saldırı vektörleri belirlenmiş ve uygun tehdit modelleme çalışmaları gerçekleştirilmiştir.
- Akıllı/endüstriyel sayaç yapısında kullanılan tüm iletişim kanalları ve protokoller (WAN, LAN vb.) belirlenmiş ve dokümante edilmiştir.
- Akıllı/endüstriyel sayaç mimarisi uçtan uca belirlenmiş ve dokümante edilmiştir. Tüm bileşenler topoloji üzerinden gösterilmiştir.

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.
- Mobil ve Akıllı Cihaz 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.

ELEKTRONİK NÜSHADIR
BASILMIŞ HALİ KONTROLSÜZ KOPYADIR

5 İLGİLİ DOKÜMANLAR

5.1 Dahili Dokümanlar

- Kapsam Analizi Dokümanı
- Varlık Yönetimi Prosedürü
- 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
- EPDK Siber Güvenlik Yetkinlik Modeli Yönetmeliği
- CBDDO Bilgi ve İletişim Güvenliği Rehberi

ELEKTRONİK NÜSHADIR
BASILMIŞ HALİ KONTROLSÜZ KOPYADIR