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; bilgi işlem kaynaklarına yerinde ve uzaktan erişim için dikkat edilmesi gereken hususları belirlemektir. Bu doküman, "Kapsam Analizi Dokümanı"nda belirtilen birimleri kapsar.

2 ROLLER VE SORUMLULUKLAR

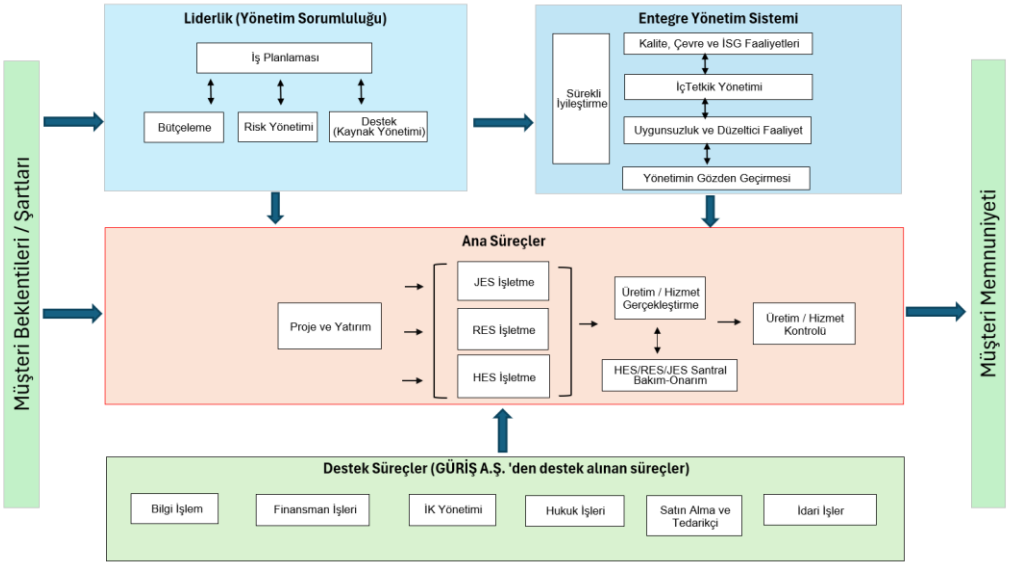
Bu dokümanla ilişkili roller ve sorumluluklar aşağıda listelenmiştir.

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

Bilgi güvenliğini sağlamanın en temel yolu, bilgi varlığına yetkisiz kişilerin erişimlerini engellemek ve yetkisi olan kişilerin erişimlerini de ihtiyaca göre kısıtlamaktır. Erişim kontrollerinde yasal gereksinimler göz önünde bulundurulur, veri sızıntısı ve yetkisiz erişimlerin önüne geçmek için uygun yetkilendirmeler yapılır. Erişimlerin takibi ve kontrolü Bilgi İşlem Müdürlüğü tarafından yapılır.

Erişim kontrolleri güvenlik duvarı ve aktif dizin sunucuları ile sağlanır. Erişim kontrolleri yapılırken 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 açıklanmıştır.

3.1. Sunucu Sistemleri Erişim Kontrolü

- Sunucu erişim yetkileri Bilgi İşlem Müdürlüğü tarafından verilir.
- Ayrıcalıklı erişim yetkileri sadece Bilgi İşlem Müdürlüğü ve talep üzerine kısa süreli yetki verilen kullanıcılarda bulunmaktadır.
- Sunucu ve hizmetlere parolasız erişim engellenmiştir.
- Sistemlere erişimlerde ortak hesap kullanılmaz.
- Sistemlere yapılan tüm erişimlerin olay kayıtları tutulur ve bozulmaya karşı korunur.
- Sistem yöneticisi rolündeki personel, sunucu ve hizmetler üzerinde her türlü işlem için tam yetkilidir.
- Sistem yöneticisi Domain Administrator hesabı ile değil Domain Administrator yetkilerine sahip başka bir hesap ile sunuculara giriş yapar.
- Sunucu erişim yetkileri Yetki Talep Formu ile birlikte Bilgi İşlem Müdürlüğü'ne e-posta yoluyla iletilir. Kısıtlamalı erişim yetkisi farklı hesap oluşturularak verilir. Personele gerekli bilgiler iletilir. İşlem tamamlandıktan sonra hesap devre dışı bırakılır.
- Yeni personel ya da var olan personel için ilgili Birim Yöneticisi'nden Yetki Talep Formu e-posta yoluyla Bilgi İşlem Müdürlüğü'ne bildirilmediği sürece Sunucu Sistemlerine erişim yasaklanmıştır.
- 3. Taraf erişimleri için kontrollü bir sunucu sistemlerinde yerel hesap açılır. Bu hesapların kontrolü Bilgi İşlem Müdürlüğü tarafından sağlanır. Tedarikçi firma erişim sağlayacağı zaman bilgi verir. Çalışma bittikten sonra hesap hesaba erişim kapatılır.

3.2. Kullanıcı Erişim Yönetimi

Yetkili kullanıcı erişimini temin etmek, sistem ve hizmetlere yetkisiz erişimi engellemek için dikkat edilmesi gereken hususlar aşağıda belirtilmiştir.

3.2.1. Kullanıcı Hesaplarının Yönetilmesi

- İstihdam edilen her kullanıcı için etki alanında kullanıcı, e-posta hesabı, sunucu erişimi ve VPN erişimi Bilgi İşlem Müdürlüğü personeli tarafından oluşturulur.
- Erişim hakları personel istihdamının sonlandırılması durumunda kaldırılır.

3.2.2. Kullanıcı Erişimine İzin Verme

- Kullanıcılara verilen yetkilerde görevlerin ayrılığı ilkesi göz önünde bulundurulur.
- E-posta hesapları Çok Faktörlü Kimlik Doğrulama Sistemi (MFA) aktif edilerek tüm personellere erişim izni verilir.
- Talep doğrultusunda SSL VPN erişimleri Token yöntemi ile izin verilmektedir.
- 3. Taraf erişimleri için SSL VPN hesabı oluşturulur. Gerekli kısıtlamalı yetkilendirme yapıldıktan sonra bilgiler firma ile e-posta yoluyla teslim edilir. Erişim sağlamaları gerektiğinde hesap aktif, çalışma bittikten sonra hesap pasif duruma alınır.

ELEKTRONİK NÜSHADIR
BASILMIŞ HALİ KONTROLSÜZ KOPYADIR

3.2.3. Ayrıcalıklı Erişim Haklarının Yönetimi

- Ayrıcalıklı erişim hakkı; Bilgi İşlem Müdürlüğü'ne verilmiştir. İlgili Birim Yöneticisi e-posta yoluyla Bilgi İşlem Müdürlüğü'nden talepte bulunur. Böylelikle ilgili personele geçici ayrıcalıklı erişim hakkı verilir.

3.2.4. Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi

- Kullanıcıların hesap bilgileri yönetimi "Parola Yönetimi Prosedürü" dokümanında tanımlandığı şekilde yapılır.
- Oluşturulan kullanıcı hesap bilgileri, kullanıcılara gereken gizlilik kurallarına dikkat edilerek bildirilir, açık metin olarak bildirilmez.
- Her kullanıcı için ilk hesap açıldığında farklı geçici parola oluşturulur. Bu şifreler güvenlik kuralları gereği dahili telefon hattı ile kendisine veya e-posta yoluyla birim amirine bildirilir.

3.2.5. Erişim Haklarının Gözden Geçirilmesi, Düzenlenmesi veya Kaldırılması

- Kullanıcının işe başlaması, işten ayrılması işlemleri İnsan Kaynakları Müdürlüğü tarafından yapılır. Personelin özlük bilgileri eBA ve aktif dizin sunucularına kaydedilmek üzere Bilgi İşlem Müdürlüğü'ne gönderilir.
- Bilgi İşlem Müdürlüğü onayı olmadan kimseye ek erişim hakkı verilmez.
- Personele görev ve yetkiler tamamlandıktan sonra görev ve yetkileri kapsamında gerçekleştirilir. Kişiye verilen yetkiler tutanaklar ile kendisine teslim edilir.
- Görev değişikliği İnsan Kaynakları Müdürlüğü tarafından Bilgi İşlem Müdürlüğüne bildirilir. Güncelleme aktif dizin ve eBA sunucularında kayıt altına alınır.
- Personelin işten ayrılması halinde, bu durum Bilgi İşlem Müdürlüğüne bildirilir. Bilgi İşlem Müdürlüğü personelle ilgili yetkilendirmeleri kaldırır.

3.3. Güvenli Oturum Açma

- Oturum açma işlemleri sırasında, yetkisiz kullanıcılara yol göstermemesi amacıyla yardım mesajları yayınlanmaz.
- Hatalı bir giriş yapıldıysa hangi verinin hatalı olduğu belirtilmez.
- Maksimum oturum açma deneme sayısı aşıldığı zaman sistemin uyarı vermesi sağlanır.
- Oturum açma işlemi için izin verilen süreler tanımlanır ve bu süre aşıldığında oturum açma istemi sonlandırılır.
- Tüm bilişim sistemlerine ya da uygulamalara parola girilirken ekranda karakterlerin görüntülenmemesi sağlanır.
- Zaman aşımı süresi, bilginin kritikliği, uygulama özellikleri ve istemcinin taşıdığı risklerin derecesine göre belirlenir.

3.4. Parola Yönetim Sistemi

Kullanıcılar tarafından kullanılan parolalar "Parola Yönetimi Prosedürü"ne uygun olarak tanımlanır.

3.5. Program Kaynak Koduna Erişim Kontrolü

Program kaynak kodunun ve kütüphanelerinin alınması ve saklanması ile ilgili hususlar şartnamelerde belirtilir. Kaynak koduna erişimlerin kısıtlanması için en az aşağıdaki adımlar göz önünde bulundurulur:

- Kaynak kod ve kütüphaneler, canlı uygulama ortamında tutulmaz.
- Personelin kaynak kod ve kütüphanelerine erişimi, ihtiyaçlara göre sınırlandırılır.
- Program kaynak kod ve kütüphanesine erişimler, Bilgi İşlem Müdürü'nün onayı olmadan yapılmaz.
- Program kaynak kod ve kütüphanesi ile ilgili değişiklikler için olay kayıtları Logsign programı üzerinde tutulur ve saklanır.
- Değişiklikler öncesi kaynak kod ve kütüphanelerinin tüm sürümleri saklanır.

ELEKTRONİK NÜSHADIR
BASILMIŞ HALİ KONTROLSÜZ KOPYADIR

4 İLGİLİ DOKÜMANLAR

4.1 Dahili Dokümanlar

- Kapsam Analizi Dokümanı
- Parola 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