

	FİZİKSEL ORTAM GÜVENLİĞİ POLİTİKASI	Doküman No	PL.09
		Yayın Tarihi	16.07.2018
		Revizyon No	02
		Revizyon Tarihi	04.07.2025
		Sayfa No	1/4

İÇİNDEKİLER

İÇİNDEKİLER	1
1 Amaç	2
2 Kapsam	2
3 Tanımlar ve Kısaltmalar	2
4 Sorumlular	2
5 Kurallar	2
5.1 Fiziksel Güvenlik Sınırı ve Çalışma Koşulları	2
5.2 Dış ve Çevresel Tehditlere Karşı Koruma	3
5.3 Ziyaretçi ve Tedarikçi Kısıtları	4
6 Yaptırım	4
7 İlgili Dokümanlar	4

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

	FİZİKSEL ORTAM GÜVENLİĞİ POLİTİKASI	Doküman No	PL.09
		Yayın Tarihi	16.07.2018
		Revizyon No	02
		Revizyon Tarihi	04.07.2025
		Sayfa No	2/4

1 Amaç

Bu politikanın amacı, ESOGÜ BİDB bünyesinde Bilgi Güvenliği Yönetim Sistemi uygulanması esnasında uyulması gereken fiziksel ortam güvenliği gereksinimlerini tanımlar.

2 Kapsam

ESOGÜ BİDB faaliyetlerinin yürütüldüğü tüm alanlar ve ilgili tüm personeller bu politika kapsamındadır.

3 Tanımlar ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi

BİDB: Bilgi İşlem Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

4 Sorumlular

Bu politikanın oluşturulmasından Bilgi Güvenliği Birimi sorumludur. Politikanın uygulanmasından tüm ESOGÜ BİDB personeli sorumludur.

Ek olarak aşağıdaki özel sorumluluklar bulunmaktadır.

5 Kurallar

5.1 Fiziksel Güvenlik Sınırı ve Çalışma Koşulları

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

	FİZİKSEL ORTAM GÜVENLİĞİ POLİTİKASI	Doküman No	PL.09
		Yayın Tarihi	16.07.2018
		Revizyon No	02
		Revizyon Tarihi	04.07.2025
		Sayfa No	3/4

- Eskişehir Osmangazi Üniversitesi Bilgi İşlem Daire Başkanlığı adresinde ESOGÜ BİDB için tanımlanmış alan BGYS'nin uygulandığı alanın fiziksel sınırlarını oluşturur.
- Bu alan kapalı duvarlarla çevrilmiş ve kampüs içerisinde olup erişim kısıtlaması uygulanmaktadır.
- Bu kapsamda ESOGÜ BİDB sınırlarına girişte kartlı geçiş denetimi uygulanır. BİDB'ye giriş yetkisi sadece BİDB personelinin kimlik kartlarına tanımlanmıştır.
- Gizlilik, bütünlük veya erişilebilirlik açısından varlık değeri yüksek olan bilgi varlıklarının bulunduğu ortamlara katmanlı erişim denetimi uygulanmaktadır. BİDB Sistem Odasına giriş yetkisi sadece BİDB Yöneticileri ve ilgili birim personelinin kurum kimlik kartlarına tanımlanmıştır.
- ESOGÜ BİDB ortamının giriş noktalarında kameralı izleme ve kayıt imkanı bulunmaktadır.
- Kamera, kartlı geçiş ve parmak izi sistemlerinin çalışabilirliği kontrol edilmelidir. Kamera izleme sistemleri Güvenlik Amirliği Birimi tarafından, kartlı geçiş sistemi Akıllı Kart Merkezi Birimi tarafından kontrol edilmektedir.
- Güvenli alanlarda çalışmak için ihtiyaç duyulan fazladan prosedür ve talimatlar BGYS Yönetim Temsilcisine bildirilmeli onun tarafından veya onun koordinasyonunda tanımlanmalıdır.

5.2 Dış ve Çevresel Tehditlere Karşı Koruma

- Vandalizm gibi fiziksel saldırılara karşı Bina girişinde veya giriş güzergâhında güvenlik görevlileri bulunmalıdır.
- Genel felaket durumlarında Kriz Durumu ve İş Sürekliliği Prosedürü içinde tanımlanan esaslara göre hareket edilmelidir.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

	FİZİKSEL ORTAM GÜVENLİĞİ POLİTİKASI	Doküman No	PL.09
		Yayın Tarihi	16.07.2018
		Revizyon No	02
		Revizyon Tarihi	04.07.2025
		Sayfa No	4/4

5.3 Ziyaretçi ve Tedarikçi Kısıtları

- ESOGÜ BİDB için dışarıdan gelen ziyaretçiler veya tedarikçiler ancak personel refakatinde ESOGÜ BİDB sınırları içerisinde dolaşabilir.
- Ziyaretçi ve tedarikçilerin bilmesi gereken kadar prensibine göre hareket etmesi sağlanmalıdır.
- Ziyaretçi ve tedarikçilere refakat etmek, personelin ziyaret sebebi ile ilgili olan personelin sorumluluğundadır.

6 Yaptırım

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Yöneticisi tarafından e-posta üzerinden yazılı olarak uyarılır. Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve Üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.

Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, Olay İhlal Yönetimi Prosedüründe tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.

7 İlgili Dokümanlar

PR.12 - OLAY İHLAL YÖNETİM PROSEDÜRÜ

PR.21 - GÜVENLİ ALANLARDA ÇALIŞMA PROSEDÜRÜ

PR.21 – FR.2 – GÜVENLİ ALANLAR KROKİSİ

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK