



# **ERZURUM BÜYÜKŞEHİR BELEDİYESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI**

## **FİZİKSEL GÜVENLİK POLİTİKASI**

(Versiyon 1.0)

2022



## FİZİKSEL GÜVENLİK POLİTİKASI

Doküman No	EBB-POL-06
Yayın Tarihi	12.12.2022
Revizyon No	
Revizyon Tarihi	
Sayfa No	2 / 6

### Doküman Detayları

Hazırlanma Tarihi	12.12.2022	Yayın	Final
Hazırlayan	Olcaç Ozan DİKBAŞ – Ersin YILDIZ		
Doküman Numarası	EBB-POL-06		

### Revizyon Geçmişi

Revizyon Tarihi	Önceki Revizyon Tarihi	Yapılan Değişikliklerin Özeti
12.12.2022		İlk Yayın

### Onay

Onaylayan	İmza	Görevi	Tarih	Versiyon
Zafer AYNALI		Genel Sekreter	12.12.2022	1.0
Murat ALTUNDAĞ		Genel Sekreter Yardımcısı	12.12.2022	1.0
Serkan ÇEKİÇ		Bilgi İşlem Daire Başkanı	12.12.2022	1.0



## FİZİKSEL GÜVENLİK POLİTİKASI

Doküman No	EBB-POL-06
Yayın Tarihi	12.12.2022
Revizyon No	
Revizyon Tarihi	
Sayfa No	3 / 6

### 1. AMAÇ

Bu politikanın amacı Erzurum Büyükşehir Belediyesi Bilgi İşlem Daire Başkanlığı'nda donanımlar üzerinde alınan yazılımsal güvenlik kadar, fiziksel güvenliğin de önemine dikkat çekmek ve iş alanına ve bilgilerine, yetkisiz erişimin, hasar ve müdahalenin engellenmesi için temel kuralları belirlemektir.

### 2. KAPSAM VE SORUMLULUKLAR

Bu politika Erzurum Büyükşehir Belediyesi Bilgi İşlem Daire Başkanlığı'nın hizmet vermesi için gerekli olan tüm donanımları, fiziksel altyapıyı, bu donanımların içinde bulunduğu ortamı ve konuyla ilgili sorumluları kapsar. Uygulanmasından tüm personel sorumludur.

### 3. UYGULAMA

#### 3.1. Donanım

- 7/24 kesintisiz çalışan sistemlere mümkün olduğunca donanımsal arıza durumunda müdahale edebilmek için, tüm donanımların hataya dayanıklılık (fault tolerance) ve sistem çalışırken değiştirilebilir (hot swap) özelliklerinin olmasına, kendi içlerinde veya birbirleriyle paralel, yedekli çalışabilir olduğuna dikkat edilecektir.
- İş sürekliliği için her donanımın aktif-aktif ya da aktif-pasif çalışan yedekli (redundant) yapıda olacaktır.
- Donanımlarda oluşabilecek parça arızaları için kritik parçalar yedeklenecek, donanım bakımları düzenli olarak belli periyotlarda yapılacaktır.

#### 3.2. İnsan – Hırsızlık -Sabotaj

- Hırsızlık ve sabotaja karşı bina güvenliği,bina girişlerinde ve katlarda kamera bulunmaktadır.
- Ofis alanları sürekli kilitli tutulmakta, sadece yetkili personel için erişim izni verilmektedir.
- Kurum binası dışına çıkarılmış gizli donanım, yazılım, dokümanlar (notebook, desktop pc, dvd, dlt, dosya vb.) umumi alanlarda, evde, arabada açıkta bırakılmayacak, mümkünse kilitli çanta, kutu vb. ile taşınacaktır.

#### 3.3. Yangın

- Donanımlar yangına karşı oldukça zayıf bir korumaya sahiptirler. Yangın sistemlere doğrudan yakarak zarar veremese bile, yüksek sıcaklık sabit disklerin ve kartlar üzerindeki tüm lehimlerin erimesine neden olabilir.
- Mümkünse ofis alanlarına ve odaya gelen tüm kablolar dışarıdan gelecek ısıyı engellemek için ısı yalıtımı yapılacak, Halogen Free kablo ve elektrik ekipmanlarının kullanılması sağlanacaktır. Bu kablolar ve korumalar yandığında alevi iletmeyerek, yangının diğer bölgelere sıçrama zamanını azaltacaktır.



## FİZİKSEL GÜVENLİK POLİTİKASI

Doküman No	EBB-POL-06
Yayın Tarihi	12.12.2022
Revizyon No	
Revizyon Tarihi	
Sayfa No	4 / 6

- Veri Merkezinde sigara içilmesi yasaktır.
- Alarm durumunda ilgili kişilere e-mail yoluyla sistemler tarafından bilgilendirme yapılacaktır. Otomatik yangın alarm sisteminin yanlış alarm ve acil durumlarda durdurulabilir olduğu denetlenecektir.
- Taşınabilir yangın söndürücülerin kapıya olabildiğince yakın olmasına dikkat edilecektir.
- Veri merkezine girme yetkisine sahip personelin yangın söndürücüyü kullanabilme konusunda yeterli deneyime sahip olması, yangın söndürücülerin doluluğunun periyodik olarak kontrol edilmesi sağlanacaktır.
- Veri merkezinde özellikle otomatik gazlı yangın söndürme sistemleri tercih edilecektir. Eğer yangın söndürme sistemi FM200 gibi gazlı bir sistem ise, yangın alarmı ile birlikte veri merkezine girecek personelin gazdan etkilenmemesi için yapması gerekenleri gösteren talimatnamenin de veri merkezinde uygun bir yere yerleştirilmesi sağlanmalıdır.

### 3.4. Sıcaklık

- Birçok donanım için 15-25 °C arası oda sıcaklıklarının korunması uygun olacaktır.
- Donanımların kullanım klavuzlarından faydalanarak uygun sıcaklık aralıkları tespit edilip (genelde 15-25 °C), klima ve iklimlendirme sistemleriyle uygun oda sıcaklığı dengelenecektir.
- Donanımlar duvarlara çok yakın yerleştirilmeyecektir. Duvarlara çok yakın yerleştirilen donanımlar, havalandırmayı engelleyerek, sistemlerin iç ısılarının yükselmesine neden olabilir. Donanımların duvarlara mesafesini belirlemek için donanımın kılavuzundan faydalanılacaktır. Kılavuzda belirtilmiyorsa donanımlar hava sirkülasyonunu sağlayacak biçimde ve en az 15-20 cm boşluk bırakacak şekilde yerleştirilmelidir.

### 3.5. Deprem Veya Patlama

- Titreşim, insanları rahatsız etmeyecek kadar az da olsa, uzun sürede bilgisayar sistemlerine zarar verebilir. En hafif titreşim bile, zamanla sabit disklerin kafa ayarlarının bozulmasına sebep olabilir.
- Donanımların, zeminden çok yükseğe yerleştirilmesinden kaçınılacaktır.
- Rack kabinlerin yere, tavana, kendi aralarında rack mount kitlerle sabitlenmesi ve içindeki tüm donanımların vidalarla ve kablo bağlarıyla sabitlenmesi sağlanacaktır.
- Donanımlar özellikle zeminin üzerindeki katlarda, pencerelerden uzak tutulacaktır.

### 3.6. Enerji Ve Kablolama

- Manyetik alan oluşumu sonucu veri kayıplarını minimize etmek için enerji ve network kabloları ayrı kanal veya ızgaralardan yapılacaktır.
- Kritik donanımlar, birbiriyle paralel çalışan, uygun kapasiteli, en az iki adet UPS'den beslenmesi sağlanacak ve UPS'lere de ayrı trafodan enerji verilecektir. Her rack kabine iki farklı UPS'den enerji verilecek, her priz sigortasının ayrı olması sağlanacak ve hangi rack kabine ait olduğu sigorta üzerinde belirtilecektir.
- Topraklamanın düzgün yapılması, UPS'ler ve Rack kabinler için şebekeden ayrı topraklama çekilmesi sağlanacaktır.



## FİZİKSEL GÜVENLİK POLİTİKASI

Doküman No	EBB-POL-06
Yayın Tarihi	12.12.2022
Revizyon No	
Revizyon Tarihi	
Sayfa No	5 / 6

- Mümkünse jeneratör kullanılacaktır. Şebeke beslemesinin kesilmesi durumunda, jeneratörün 2-5 sn içinde otomatik devreye girmesi sağlanacak, UPS'ler jeneratör üzerinden beslenmeye devam edecektir.
- Statik elektriğin yaratabileceği sorunlara engel olmak üzere teknik servis tezgahına gerekli fiziksel önlemler alınacaktır.
- Yedekler manyetik ortamlarda saklandığı durumlarda, yedeklerin binanın iskeletini oluşturan demirlerden olabildiğince uzakta olması sağlanacaktır.
- Paratoner kablolarının ofis alanından uzak olacak biçimde yapılmasını sağlanacaktır
- Ethernet kartları ve switch portlarına giden patch paneller portları bina data uçları ile aynı olacak şekilde etiketlenmeli, mümkünse farklı vlan'lar için farklı renkte kablolar kullanılmalı, uç terminasyon yapısı switchlerin üzerine etiketlenerek yapılandırılmalıdır.

### 3.7. Nem

- Nemin çok az olması, statik elektrik yüklenme ve aktarımlarını artırarak manyetik teyp ve benzeri bileşenlerde sorunlara yol açacaktır. Nem oranının çok yükselmesi ise, bilgisayar sistemlerinin devrelerinde kısa devrelere kadar uzanan sorunlara neden olabilecektir.
- Nem düzeyi %40 ile %75 arasında tutulacaktır.
- Donanımların nem duyarlılığı birbirlerinden farklı olabilir. Uygun nem düzeyinin tespiti için donanımların kullanım kılavuzlarına bakılacaktır.
- Klima veya iklimlendirme sistemlerinin ofis alanı gibi kurum kritik bölgelerinde sürekli çalışır durumda olduğu sağlanacaktır.
- Kritik bölgelerdeki iklimlendirme sistemlerini sürekli izlemeye tabi tutulacaktır.

### 3.8. Su

- Su, aktif sistemleri çok hızlı biçimde çalışmaz hale getirebilir. Su ile ilgili en büyük tehlike, elektriksel bir kısa devredir.
- Veri merkezinde iki farklı seviyede su dedektörleri kullanılmalıdır.
- Alarm durumunda ilgili kişilere e-posta ve/veya SMS yoluyla alarmların ulaşması sağlanacaktır.
- Rack kabinler klima altlarına konulmayacaktır.

### 3.9. Toz

- Toz disk kafalarında, optik, manyetik ortam ürünlerinde, fanlarda birikerek sistemi çalışmaz hale getirebilir. Elektronik ortamlar üzerinde biriken toz parçacıkları, kısa devrelere, sistemlerin iç sıcaklıklarının artmasına neden olmakta ve sistemlere zarar vermektedir.
- Ofis alanı ve veri merkezi belirli aralıklarla tozdan arındırılacaktır.
- Klima, havalandırma sistemlerinin periyodik bakımlarının yapılması, filtrelerinin temizlenmesi sağlanacaktır.
- Ofis alanındaki havalandırma sürekli sağlanacaktır.



## FİZİKSEL GÜVENLİK POLİTİKASI

Doküman No	EBB-POL-06
Yayın Tarihi	12.12.2022
Revizyon No	
Revizyon Tarihi	
Sayfa No	6 / 6

- Eğer sunucu ve aktif cihazların üzerinde de hava filtreleri varsa, periyodik olarak değiştirilmesi sağlanacaktır. Cihazların en az yılda bir hava kompresörü yardımıyla temizlenmesi ve bakımlarının yapılması sağlanacaktır.

### 3.10. Böcekler Ve Kemirgenler

- Böcekler ve kemirgenler (fareler), ofis alanlarında özellikle yükseltilmiş döşeme ve rack kabinler içerisinde, sıkışık kablo tomarlarının arasında görülebilirler. Anahtarlı güç kaynağının anahtar aksamına sıkışıp kalmış bir böcek; enerji kablosunu kemirmiş bir fare aktif sistemi kısa sürede çalışmaz hale getirebilir.
- Böceklerden ve kemirgenlerden korunmak için veri merkezinde gerekli kontroller yapılacaktır.

### 4. YAPTIRIM

Bu politikaya uygun olarak çalışmayan tüm personel hakkında Disiplin Prosedürü hükümleri uygulanır.

### 5. İLGİLİ DOKÜMANLAR

- İŞ SÜREKLİLİĞİ-ACİL VE BEKLENMEDİK DURUM PLANI ( EBB-PL-01 )