

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı Sistem Odası Fiziksel alanları Güvenlik Politikası	Doküman No	PLT-031
		İlk Yayın Tarihi	6.12.2024
		Revizyon Tarihi	6.12.2024
		Revizyon No	000
		Sayfa No	1 / 5

1. AMAÇ

Bu politikanın amacı Süleyman Demirel Üniversitesi fiziksel yerleşkelerinin güvenliğinin önemine dikkat çekmek ve yetkisiz erişimin, hasar ve müdahalenin engellenmesi için temel kuralları belirlemektir.

2. KAPSAM

Bu politika Süleyman Demirel Üniversitesi'nin hizmet vermesi için gerekli olan tüm donanımları, fiziksel altyapıyı, bu donanımların içinde bulunduğu ortamı ve konuyla ilgili sorumluları kapsar.

3. SORUMLULUKLAR

Uygulanmasından tüm ağ ve sistem birimi personelleri sorumludur.

4. UYGULAMA

4.1. Giriş Kontrolleri

- İlgili Sistem odalarına girişler sadece BİDB tarafından yetkilendirilmiş personellerce yapılmalıdır.
- Sistem odalarına giriş için ilk dış kapı geleneksel anahtar yöntemi ile erişim sağlanmalıdır. Kişi anahtar ile kapıyı açsa dahi kartını okutmadan yetkili alana giriş yapamamaktadır.
- İlgili sistem odalarının kart okuyucuları yetkilendirilmesi yerel olarak yapılmaktadır.
- İlgili giriş çıkışların kayıtları elektronik ve kapılarda bulunan kağıt çizelgelere alınmaktadır.

4.2. Donanım

- 7/24 kesintisiz çalışan sistemlerde, donanımsal arıza durumuna müdahale edebilmek için tüm donanımların hataya dayanıklı (faul tolerance) ve sistem çalışırken değiştirilebilir (hot swap) özelliklerinin olmasına, kendi içlerinde veya birbirleriyle paralel, yedekli çalışabilir olduğuna dikkat edilmelidir.
- İş sürekliliği için donanımlar, aktif-aktif ya da aktif-pasif çalışan yedekli (redundant) yapıda olmalıdır.
- Donanımlarda oluşabilecek parça arızaları için kritik parçalar yedeklenmeli, donanım bakımları düzenli olarak belli periyotlarda yapılmalıdır.

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekai KÜNAR	Doktor Öğretim Üyesi - Veli ÇAPALI

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı Sistem Odası Fiziksel alanları Güvenlik Politikası	Doküman No	PLT-031
		İlk Yayın Tarihi	6.12.2024
		Revizyon Tarihi	6.12.2024
		Revizyon No	000
		Sayfa No	2 / 5

4.3. İnsan – Hırsızlık -Sabotaj

- Hırsızlık ve sabotaja karşı bina güvenliği, kritik bölgelere kart tanıma sistemi ve ek anahtarlı giriş, bina girişlerinde ve katlarda kamera bulunmalıdır.
- Sistem odaları sürekli kilitli tutulmalı, sadece yetkili personel için erişim izni verilmelidir.
- Fiziksel yerleşke dışına çıkarılmış gizli donanım, yazılım, dokümanlar (notebook, desktop pc, dvd, dlt, dosya vb.) umumi alanlarda, evde, arabada açıkta bırakılmamalı, mümkünse kilitli çanta, kutu vb. ile taşınmalıdır.
- Kişisel verilerin, Veri Sorumlusu hakimiyet alanı dışına çıkarılmamaları için merkezi bir dosya sunucusunda her kullanıcı için ana klasör yapısı kurulmalı, gerekirse istemcilerde domain veya lokal politikalarla usb, com vb. türü tüm portlar, dvd-rom, disk drive, usb memory vb. gibi medya araçlarının ve lokal sürücülerin tümünün kullanımı kapatılmalıdır.

4.4. Yangın

- Sistem odalarına ve odaya gelen tüm kablolar dışarıdan gelecek ısıyı engellemek için ısı yalıtımı yapılmalı, Halojen Free kablo ve elektrik ekipmanlarının kullanılması sağlanmalıdır. Bu kablolar ve korumalar yandığında alevi iletmeyip, yangının diğer bölgelere sıçrama zamanını azaltacaktır.
- Sistem odasında sigara içilmemelidir.
- Sistem odasındaki yangın ve duman detektörlerinin çalışır durumda olduğu periyodik tatbikatlar ile kontrol edilmelidir.
- Alarm durumunda ilgili kişilere e-posta, SMS, telefon vb. yollarıyla alarmların ulaşması sağlanmalıdır. Otomatik yangın alarm sisteminin yanlış alarm ve acil durumlarda durdurulabilir olduğu denetlenmelidir.
- Taşınabilir yangın söndürücülerin kapıya olabildiğince yakın olmasına dikkat edilmelidir.
- Sistem odasına girme yetkisine sahip personel yangın söndürücüyü kullanabilme konusunda yeterli deneyime sahip olmalı, yangın söndürücülerin doluluğu periyodik olarak kontrol edilmelidir.
- Sistem odasında özellikle otomatik gazlı yangın söndürme sistemleri tercih edilmelidir. Eğer yangın söndürme sistemi CO₂, FM200, NAF-S-III, Halon gibi gazlı bir sistem ise, yangın alarmı ile sistem odasına girecek personelin gazdan etkilenmemesi için yapması gerekenleri gösteren uyarı panosunun da sistem odasının dış kapısına ya da uygun bir yere yerleştirilmesi

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekai KÜNAR	Doktor Öğretim Üyesi - Veli ÇAPALI

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı Sistem Odası Fiziksel alanları Güvenlik Politikası	Doküman No	PLT-031
		İlk Yayın Tarihi	6.12.2024
		Revizyon Tarihi	6.12.2024
		Revizyon No	000
		Sayfa No	3 / 5

sağlanmalıdır.

- Cep telefonları, telsizler, her türlü radyo alıcı ve vericileri bilgisayar sistemlerine zarar verir. Özellikle güçlü vericiler, bilgisayar sistemlerine kalıcı zararlar verebilirler. Bazı gazlı yangın söndürücü sistemleri, alıcı-vericilerin yakın çevresinde iken patlama eğilimi gösterebilirler. Bu tür yangın söndürücülerin bulunduğu ortamlarda kesinlikle alıcı ve vericiler kullanılmayacaktır. Her türlü alıcı ve verici, bilgisayar sistemlerinden, kablolardan ve çevre birimlerinden en az 2,5 m uzakta tutulacaktır.

4.5. Sıcaklık

- Birçok donanım için 10-25 °C arası oda sıcaklıklarının korunması uygun olacaktır.
- Donanımların kullanım kılavuzlarından faydalanarak uygun sıcaklık aralıkları tespit edilip (genelde 20-25 °C), klima ve iklimlendirme sistemleriyle uygun oda sıcaklığı dengelenmelidir.
- Sistem odasına termal ısı detektörleri yerleştirerek çok sıcak ve çok soğuk durumlarda alarmların oluşturulması sağlanacaktır. Alarm durumunda ilgili kişilere e-posta, SMS, telefon vb. yollarla alarmların ulaşması sağlanmalıdır.
- Donanımlar duvarlara çok yakın yerleştirilmemelidir. Duvarlara çok yakın yerleştirilen donanımlar, havalandırmayı engelleyerek, sistemlerin iç ısılarının yükselmesine neden olabilir. Donanımların duvarlara mesafesini belirlemek için donanımın kılavuzundan faydalanılmalıdır. Kılavuzda belirtilmiyorsa donanımlar hava sirkülasyonunu sağlayacak biçimde ve en az 15-20 cm boşluk bırakacak şekilde yerleştirilmelidir.

4.6. Deprem veya Patlama

- Donanımların, zeminden çok yükseğe yerleştirilmesinden kaçınılmalıdır.
- Kabinetlerin yere, tavana, kendi aralarında ek aparatlar ile sabitlenmesi ve içindeki tüm donanımların vidalarla ve kablo bağlarıyla sabitlenmesi sağlanmalıdır.
- Donanımlar özellikle zeminin üzerindeki katlarda, pencerelerden uzak tutulmalıdır.
- Yedekler patlamaya ve depreme dayanabilecek kasalar içerisinde veya Süleyman Demirel Üniversitesi dışındaki başka güvenli mekanlarda saklanmalıdır.

4.7. Enerji ve Kablolama

- Sistem odalarındaki kabinler mümkün olduğunca enerji panolarından uzak noktaya konulmalıdır.
- Manyetik alan oluşumu sonucu veri kayıplarını minimize etmek için enerji ve network

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekai KÜNAR	Doktor Öğretim Üyesi - Veli ÇAPALI

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı Sistem Odası Fiziksel alanları Güvenlik Politikası	Doküman No	PLT-031
		İlk Yayın Tarihi	6.12.2024
		Revizyon Tarihi	6.12.2024
		Revizyon No	000
		Sayfa No	4 / 5

kabloları ayrı kanal veya ızgaralardan yapılmalıdır.

- Kritik donanımların, birbiriyle paralel çalışan, uygun kapasiteli, en az iki adet UPS(kesintisiz güç kaynağı)’den beslenmesi sağlanmalı ve UPS'lere de 2 farklı trafodan enerji verilecektir. Her kabine iki farklı UPS’den enerji verilmeli, her prizın sigortasının ayrı olması sağlanmalı ve hangi kabine ait olduğu sigorta üzerinde belirtilmelidir.
- Topraklamanın düzgün yapılması amacıyla UPS’ler ve kabinler için şebekeden ayrı topraklama çekilmesi sağlanmalıdır.
- Mümkünse Jeneratör kullanılmalıdır. Şebeke beslemesinin kesilmesi durumunda, jeneratörün 2-5 sn. içinde otomatik devreye girmesi sağlanmalı, UPS’ler jeneratör üzerinden beslenmeye devam etmelidir. UPS’in şebeke enerjisini düzenleyemediği edemediği durumlarda ek regülatörlerin kullanılması sağlanmalıdır.
- Statik elektriğin yaratabileceği sorunlara engel olmak üzere sistem odası zeminine yada kabinlere gerekli fiziksel önlemler alınacaktır.
- Yedeklerin manyetik ortamlarda saklandığı durumlarda, yedeklerin binanın iskeletini oluşturan demirlerden olabildiğince uzakta olması sağlanmalıdır.
- Paratoner kablolarının sistem odasından uzak olacak biçimde yapılmasını sağlanacaktır
- Ethernet kartları ve switch portlarına giren ara(patch) kablolar network topoloji şemasında belirtilen uç terminasyonuna göre etiketlenmelidir.

4.8. Nem

- Nem düzeyi %20 ile %50 arasında tutulmalıdır.
- Donanımların nem duyarlılığı birbirlerinden farklı olabilir. Uygun nem düzeyinin tespiti için donanımların kullanım kılavuzlarına bakılacaktır.
- Klima veya iklimlendirme sistemleri, sistem odası gibi kritik bölgelerin sürekli çalışır durumda olmalıdır.
- Kritik bölgelerdeki iklimlendirme sistemlerini sürekli izlenmesi gerekmektedir.

4.9. Su

- Sistem odasında iki farklı seviyede su detektörleri kullanılmalıdır.
- Alarm durumunda ilgili kişilere e-posta, SMS, telefon vb. yollarla alarmların ulaşması sağlanacaktır.

4.10. Toz

- Sistem odası belirli aralıklarla tozdan arındırılmalıdır.

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekai KÜNAR	Doktor Öğretim Üyesi - Veli ÇAPALI

	SÜLEYMAN DEMİREL ÜNİVERSİTESİ Bilgi İşlem Daire Başkanlığı Sistem Odası Fiziksel alanları Güvenlik Politikası	Doküman No	PLT-031
		İlk Yayın Tarihi	6.12.2024
		Revizyon Tarihi	6.12.2024
		Revizyon No	000
		Sayfa No	5 / 5

- Klima ve havalandırma sistemlerinin periyodik bakımlarının yapılması, filtrelerinin temizlenmesi sağlanmalıdır.
- Sistem odası sürekli havalandırılmalıdır.
- Eğer sunucu ve aktif cihazların üzerinde de hava filtreleri varsa, periyodik olarak değiştirilmelidir.

4.11. Böcekler ve Kemirgenler

- Böceklerden ve kemirgenlerden korunmak için belirli aralıklarla ilaçlama yapılacaktır.

5. YAPTIRIM

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

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekai KÜNAR	Doktor Öğretim Üyesi - Veli ÇAPALI