1. AMAÇ

Bu politikanın amacı, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında bilgi varlıklarının bulunduğu sistem odaları ve kritik fiziksel alanların; yetkisiz erişim, fiziksel müdahale, hırsızlık, sabotaj, yangın, su baskını, aşırı sıcaklık/nem, enerji kesintisi, deprem ve benzeri çevresel tehditlere karşı korunmasına yönelik temel kuralları belirlemektir.

Bu politika ile bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunması, hizmet sürekliliğinin desteklenmesi ve fiziksel güvenlik risklerinin azaltılması amaçlanmaktadır.

2. KAPSAM

- Süleyman Demirel Üniversitesi Daire Başkanlıkları,
- Genel Sekreterlik,
- Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi,

bünyesinde bulunan ve bilgi işleme faaliyetlerinin yürütüldüğü;

- sistem odalarını,
- sunucu odalarını,
- network/iletişim odalarını,
- kritik bilgi işlem altyapısının bulunduğu alanları,
- bilgi ve iletişim teknolojileri ekipmanlarının bulunduğu kontrollü alanları,
- bu alanlarda bulunan sunucu, ağ cihazı, güvenlik cihazı, depolama sistemleri, UPS, yedekleme sistemleri ve benzeri bilgi varlıklarını, ve bu alanlara erişimi bulunan personel, hizmet sağlayıcılar ve diğer ilgili tarafları kapsar.

3. SORUMLULUKLAR

3.1. Bilgi İşlem Daire Başkanlığı;

- sistem odalarının fiziksel ve çevresel güvenlik kontrollerinin koordinasyonundan,
- erişim yetkilerinin yönetilmesinden,
- sistem odalarında bulunan bilgi varlıklarının uygun şekilde korunmasından,
- çevresel izleme ve alarm mekanizmalarının işletilmesinden,
- kritik altyapının bakım ve kontrollerinin planlanmasından,
- fiziksel güvenlik olaylarının ilgili süreçlere aktarılmasından sorumludur.

3.2. Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi

Hastane Bilgi İşlem Birimi, kendi sorumluluğundaki sistem odaları ve kritik bilgi işlem alanlarının bu politika ve ilgili EYS dokümanlarına uygun şekilde işletilmesinden sorumludur.

3.3. Daire Başkanlıkları ve Genel Sekreterlik

Kendi sorumluluk alanlarında bulunan bilgi işlem ekipmanlarının ve kritik fiziksel alanların güvenliğinin sağlanması, erişim yetkilerinin kontrol edilmesi ve tespit edilen fiziksel güvenlik risklerinin ilgili birimlere bildirilmesinden sorumludur.

Hazırlayan	Kontrol	Onay
Sürekli İşçi - Merve GÜNEŞ	Şube Müdürü - Zekai KÜNAR	Doç. Dr. - Mevlüt ERSOY

3.4. Tüm Çalışanlar ve Yetkili Kullanıcılar

Çalışanlar ve yetkili kullanıcılar;

- yetkisiz kişilerin kontrollü alanlara girişine izin vermemek,
- kendilerine verilen erişim yetkilerini başkalarıyla paylaşmamak,
- fiziksel güvenlik ihlallerini veya şüpheli durumları bildirmek,
- taşınabilir bilgi varlıklarını fiziksel tehditlere karşı korumak ile yükümlüdür.

4. UYGULAMA

4.1. Fiziksel Güvenlik Alanlarının Belirlenmesi

- Sistem odaları ve kritik bilgi işlem alanları fiziksel güvenlik gereksinimlerine göre belirlenir ve yetkisiz kişilerin erişimini önleyecek şekilde korunur.
- Kritik alanlara erişim yetkileri görev ve sorumluluklar dikkate alınarak belirlenir.
- Sistem odaları mümkün olduğunca yetkisiz kişilerin erişimine kapalı ve sürekli kontrollü tutulur.
- Sistem odalarında kullanılan fiziksel güvenlik önlemleri; alanın kritiklik düzeyi, barındırılan bilgi varlıklarının niteliği, risk değerlendirmesi ve teknik gereksinimler dikkate alınarak belirlenir.

4.2. Giriş ve Erişim 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.
- Erişim yetkileri düzenli olarak gözden geçirilir ve görev değişikliği, birim değişikliği veya işten ayrılma durumlarında gerekli erişim yetkileri zamanında kaldırılır veya güncellenir.
- Yetkisiz kişilerin sistem odalarına refakatsiz girmesine izin verilmez.
- Hizmet sağlayıcı, bakım personeli ve diğer dış tarafların erişimleri görev, süre ve alan bazında sınırlandırılır ve gerektiğinde refakat altında gerçekleştirilir.
- Sistem odası anahtarları, kartları ve diğer fiziksel erişim araçları yetkisiz kişilere devredilemez.

4.3. Ziyaretçi ve Üçüncü Taraf Erişimi

- Ziyaretçilerin sistem odalarına girişleri görev gerekliliği ile sınırlandırılır.
- Üçüncü tarafların bakım, kurulum, onarım veya teknik destek amacıyla gerçekleştirdiği erişimler mümkün olduğunca önceden yetkilendirilir.
- Kritik sistemlere müdahale gerektiren işlemlerde ilgili personelin gözetimi sağlanır.
- Gerektiğinde ziyaretçi giriş-çıkış kayıtları tutulur.

4.4. Fiziksel Güvenlik İzleme

- Kritik alanlarda risk değerlendirmesine uygun olarak kamera, kartlı geçiş, alarm, sensör ve benzeri fiziksel güvenlik kontrolleri uygulanabilir.
- Kamera ve erişim kayıtları ilgili mevzuat, KVKK ve kurumun kayıt yönetimi kurallarına uygun şekilde korunur.

- Fiziksel güvenlik sistemlerinin çalışırlığı ve kritik alarm mekanizmaları belirlenen periyotlarda kontrol edilir.
- Fiziksel güvenlik olayları ilgili Olay Yönetimi ve/veya Düzeltici Faaliyet süreçlerine aktarılır.

4.5. Donanım ve Altyapının Korunması

- Kritik bilgi işlem ekipmanları; yetkisiz müdahale, devrilme, düşme, çarpma ve benzeri fiziksel risklere karşı uygun şekilde konumlandırılır ve gerektiğinde sabitlenir.
- Kritik sistemlerde donanım yedekliliği ve hata toleransı, hizmetin kritiklik seviyesi ve risk değerlendirmesi doğrultusunda planlanır.
- Kritik donanımlarda meydana gelebilecek arızalara karşı gerekli yedek parça, yedek sistem veya alternatif çalışma yöntemleri belirlenir.
- Donanım bakım faaliyetleri üretici tavsiyeleri, teknik gereksinimler ve kurumun bakım planları doğrultusunda gerçekleştirilir.
- Donanımların fiziksel yerleşimi, hava akışı ve bakım erişimini engellemeyecek şekilde planlanır.
- 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.

4.6. Taşınabilir Bilgi Varlıklarının Fiziksel Güvenliği

- Sistem odası veya kurum dışına çıkarılan notebook, taşınabilir disk, USB bellek, yedekleme medyası ve benzeri bilgi varlıkları yetkisiz erişim, kayıp, hırsızlık ve fiziksel hasara karşı korunur.
- Bilgi varlıklarının kurum dışına çıkarılması ilgili yetkilendirme ve zimmet süreçlerine uygun olarak gerçekleştirilir.
- Gizli, Çok Gizli veya kişisel veri içeren bilgi varlıklarının kurum dışına çıkarılması halinde ilgili sınıflandırma, erişim, şifreleme ve fiziksel güvenlik kuralları uygulanır.
- Taşınabilir ortamların kullanımı ve imhasında ilgili **Taşınabilir Ortam ve Cihaz Politikası** ile **Taşınabilir Ortamın İmhası Politikası** hükümleri uygulanır.

4.7. 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.

4.8. Yangın ve Duman Güvenliği

- Sistem odalarına ve odaya gelen tüm kablolara 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 CO^2, 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 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.

4.9. Deprem, Patlama ve Diğer fiziksel Tehditler

- Sistem odalarının ve bilgi işlem ekipmanlarının deprem, titreşim, yapısal hasar ve benzeri fiziksel tehditlere karşı dayanıklılığı risk değerlendirmesinde dikkate alınır.
- Kabinetler ve kritik ekipmanlar gerektiğinde devrilmeye karşı uygun şekilde sabitlenir.
- Yedekleme ortamları ve kritik bilgi varlıkları, iş sürekliliği gereksinimleri doğrultusunda ana sistemlerden bağımsız veya alternatif güvenli bir ortamda bulundurulabilir.
- Kritik yedeklerin korunmasında yangın, su baskını, deprem, hırsızlık ve benzeri riskler dikkate alınır.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.

4.10. Enerji, UPS ve Kablolama

- Sistem odalarındaki kabinler mümkün olduğunca enerji panolarından uzak noktaya konulmalıdır.
- Manyetik alan oluşumu sonucu veri kayıplarını minimize etmek için enerji ve network kablolaması 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 prizin sigortasının ayrı olması sağlanmalı

ve hangi kabine ait olduğu sigorta üzerinde belirtilmelidir.

- UPS ve enerji sistemlerinin kapasite, bakım ve çalışma durumları belirlenen periyotlarda kontrol edilir.
- 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 kablolamasının sistem odasından uzak olacak biçimde yapılmasını sağlanacaktır
- Ethernet kartları ve switch portlarına giren ara(patch) kablolar network topoloji şemasında belirtilen uç terminasyonuna göre etiketlenmelidir.

4.11. Sıcaklık ve Nem Kontrolü

- 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.
- 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.
- Kritik eşiklerin aşılması halinde ilgili personele alarm veya bildirim gönderilmesi sağlanır.
- İklimlendirme sistemlerinin bakım ve kontrolleri belirlenen periyotlarda gerçekleştirilir.

4.12. Su ve Su Baskınına Karşı Koruma

- Sistem odalarının su baskını ve su sızıntısı riskleri değerlendirilir.
- Sistem odasında iki farklı seviyede su detektörleri kullanılmalıdır.
- Alarm durumunda ilgili kişilere e-posta, SMS, telefon vb. yollarla alarmların ulaşması sağlanacaktır.
- Eğer sunucu ve aktif cihazların üzerinde de hava filtreleri varsa, periyodik olarak değiştirilmelidir.
- Su algılama alarmı oluşması halinde ilgili personelin bilgilendirilmesi ve gerekli müdahalenin

gerçekleştirilmesi sağlanır.

4.13. Toz, Böcekler ve Kemirgenlere Karşı Koruma

- Sistem odalarının temizliği belirlenen periyotlarda gerçekleştirilir.
- Klima, havalandırma ve filtre sistemlerinin bakım ve temizlikleri planlı olarak gerçekleştirilir.
- Sistem odalarında böcek ve kemirgenlerin bilgi işlem ekipmanlarına zarar vermesini önlemek amacıyla gerekli fiziksel ve teknik önlemler alınır.
- Gerektiğinde yetkili hizmet sağlayıcılar aracılığıyla ilaçlama ve benzeri koruyucu faaliyetler gerçekleştirilir.

4.14. Bakım, Onarım ve Fiziksel Müdahaleler

- Sistem odalarında gerçekleştirilecek bakım, onarım, kurulum ve değişiklik faaliyetleri yetkili personel veya yetkilendirilmiş hizmet sağlayıcılar tarafından gerçekleştirilir.
- Kritik sistemlerde gerçekleştirilecek fiziksel müdahaleler gerektiğinde değişiklik yönetimi kapsamında planlanır.
- Bakım veya onarım sırasında bilgi varlıklarının güvenliği ve kişisel verilerin korunması sağlanır.
- Kullanım dışı bırakılan cihaz ve ortamların yeniden kullanım veya imha işlemleri ilgili varlık yönetimi ve imha süreçlerine uygun olarak gerçekleştirilir.

4.15. Acil Durumlar ve Olay Yönetimi

Yangın, su baskını, aşırı sıcaklık/nem, enerji kesintisi, fiziksel saldırı, hırsızlık, sabotaj veya benzeri olaylarda;

- ilgili personel bilgilendirilir,
- can güvenliği önceliklendirilir,
- gerekli acil durum prosedürleri uygulanır,
- bilgi varlıklarının zarar görmesini önleyici tedbirler alınır,
- olay gerektiğinde Olay Yönetimi, İş Sürekliliği ve Düzeltici Faaliyet süreçlerine aktarılır.

5. YAPTIRIM

Bu politikaya aykırı hareket eden çalışanlar ve diğer ilgili taraflar hakkında, olayın niteliğine göre ilgili EYS süreçleri, sözleşme hükümleri, ilgili mevzuat ve kurumun disiplin hükümleri uygulanır.