

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	FİZİKSEL ve ÇEVRESEL GÜVENLİK PROSEDÜRÜ	Doküman No	BGYS-PR19
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	16.09.2024
		Revizyon No	02
		Sayfa No	1 / 5

1. AMAÇ

Bu prosedür, Birimimiz Bilgi Güvenliği Yönetim Sistemi kapsamındaki bilgi varlıklarının ve kaynaklarının bulunduğu fiziksel ortamın güvenlik yapısını tanımlar.

2. SORUMLULUKLAR

Bu prosedür Birimimiz çalışanlarının sorumluluğundadır.

3. UYGULAMA

Prosedürün uygulama etkinliğinin izlenmesi için yılda 1 kere fiziksel ve çevresel güvenlik değerlendirmesinin yapıldığı 'BGYS-FRM24 Fiziksel ve Çevresel Güvenlik Değerlendirme Formu' doldurulur.

4. YAPILANDIRMA

Çalışma Bölgesi ve dış çevre arasında güvenlik kapıları haricinde içeriden dışarıya herhangi bir geçişin sağlandığı bir boşluk yoktur.

Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınmalı ve uygulanmalıdır.

Yedeklenmiş materyal ve yedek sistemler ana tesisten yeterince uzak bir yerde konuşlandırılmış olmalıdır.

Veri taşıyan ya da bilgi hizmetlerini destekleyen elektrik ve haberleşme kablolarının kesilme ya da hasarlardan korunması için kablo kanalları kullanılır.

5. ERİŞİM KONTROL

Kullanıcı bilgisayar ve mobil cihazları Aktif Dizin Sistemleri ile entegre olarak çalışır ve kullanıcılar bu cihazlarına BGYS-PL01 Bilgi Güvenliği Politikası/ Parola Koruma Politikasında belirtilen şifreleme yöntemi ile erişim sağlar.

6. FİZİKSEL GİRİŞ KONTROLLERİ

- Ziyaretçilerin giriş çıkış kayıtları saklanmalıdır.
- Önceden yetkilendirilmemiş kişilerin giriş çıkışları yetkililer tarafından kontrol edilmelidir. Yetkisiz kişilerin sadece erişmesi gereken alanlara ulaşması refakat edilerek sağlanmalıdır.
- Güvenli alanlara girişler yetkili bir makam tarafından onaylanmalıdır.
- Ziyaretçilere fiziksel güvenlik ve acil durumlar hakkında bilgi verilmelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	FİZİKSEL ve ÇEVRESEL GÜVENLİK PROSEDÜRÜ	Doküman No	BGYS-PR19
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	16.09.2024
		Revizyon No	02
		Sayfa No	2 / 5

- Kayıt defteri ve elektronik izler saklanmalıdır.
- Personeller ve ziyaretçiler farklı kimlik kartları ile erişim sağlamalı, gizli alanlarda yetkisiz kişilerin görülmesi durumunda uyarı yapılmalıdır.

Birimimiz fiziksel güvenliği için aşağıdaki yöntemleri kullanmaktadır.

- a) Bina girişinde güvenlik personelleri
- b) X-Ray Cihazı
- c) Kartlı geçiş turnikeleri
- d) Yüz tanıma ve parmak okuma sistemli birime giriş kapıları
- e) Veri Merkezi için parmak izi okumalı giriş kapıları
- f) Veri Merkezi içindeki hücrelere giriş için parmak izi okumalı giriş kapıları
- g) Yangın Söndürme Sistemi
- h) Isı ve nem ve gaz sensörleri
- i) Güvenlik kameraları (Kayıtlar Destek Hizmetleri Dairesi Başkanlığı prosedürlerine göre saklanmaktadır.)
- j) Yangın Söndürme Tüpleri

7. OFİSLERİN VE ODALARIN GÜVENLİĞİ

- Ofisler ve odaların bulunduğu koridorlara erişimler kontrollü olmalıdır ve yalnızca yetkili kişiler girebilmelidir.
 - Hassas odaların tabela ve işaretleyiciler ile yerlerinin belirlenmemesi, telefon rehberleri tanıtım kitapları yetkisiz kişilerin eline geçmeyecek yerlerde saklanmalıdır.
 - Diğer Kurum çalışanları ve 3. Tarafların personel odalarına erişimlerinde yetkili çalışanlar refakat etmelidir.
 - Personel güvenliği ve sağlığı ile ilgili yönetmelikler uygulanmalıdır.
 - Personel odalarının bulunduğu koridorlarda ofisler ve odalara giriş çıkışları kaydedecek şekilde güvenlik kameraları olmalıdır.
 - Personel odada bulunmadığı zaman kapılar kilitlenmelidir. Anahtar personelde ve yedek anahtarı ilgili Şube Müdüründe bulunmalıdır.
 - Ofisler ve odalarda temiz masa temiz ekran politikasına uygun şekilde davranılmalıdır.
 - Kritik bilgi içeren ofisler ve odalar ile ilgili aşağıdaki hususlara ayrıca dikkat edilmelidir;
- a. Kritik bilgi içeren ofisler ve odalar kolay erişilebilir yerlerde konumlandırılmamalıdır,
 - b. Kritik bilgi içeren ofisler ve odalar için işaret, tabela vb. bulunmamasına dikkat edilmelidir,
 - c. Kritik bilgi içeren odalar içeride yetkili birisi olmadığı zaman kilitli tutulmalıdır. Anahtar personelde ve uygun ise yedek anahtarı güvenlikte bulunmalıdır,
 - d. Kritik bilgi içeren odalara erişimlerde mümkünse ayrıca giriş kontrolleri (parmak izi, damar okuyucu, kartlı geçiş vb.) uygulanmalıdır ve bu erişim kayıtları saklanmalıdır ve değiştirilmeye karşı korunmalıdır,

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	FİZİKSEL ve ÇEVRESEL GÜVENLİK PROSEDÜRÜ	Doküman No	BGYS-PR19
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	16.09.2024
		Revizyon No	02
		Sayfa No	3 / 5

- e. Kritik bilgi içeren ofisler ve odalarda kolay tutuşabilir malzemeler bulundurulmamalıdır,
- f. Kritik bilgi içeren ofisler ve odalarda yangın, su baskını, deprem, patlama, sivil gösteri ve hareketler ve diğer doğal veya insan kaynaklı felaketlerin muhtemel sonuçları değerlendirilmelidir ve gerekli önlemler alınmalıdır,
- g. Kritik bilgilerin sakladığı dolaplar vs. yangına dayanıklı olmalıdır.

8. SİSTEM ODALARININ GÜVENLİĞİ

- Sistem odalarına yetkisiz personelin girişi engellenmelidir.
- Girişler için sadece tek giriş bulunmalıdır ve girişlerde gerekli güvenlik tedbirleri (kartlı sistem, parmak izi vb.) alınmış olmalıdır.
- Bilgi İşlem Dairesi Başkanlığı tarafından sistem odasına girme yetkisi verilir. BGYS-LST01 Veri merkezi Giriş ve Çıkış Yetkili Listesi oluşturulmuş ve ortalama 6 aylık periyotlarla kontrol edilmektedir.
- Yetkisiz erişim tespit edildiğinde güvenlik amirliği ile irtibata geçilir.
- Kurumun sistem odası olarak kullanılacak odalarda dışarıdan görülecek pencere veya balkon kapısı bulunmamalıdır.
- Sistem odaları 7/24 güvenlik kameraları ile gözetlenmeli ve 30 günlük kayıt saklanmalıdır.
- Sistem odalarında bulunan iklimlendirme sistemlerinden sızan su sızıntıları, sıcaklık, yangın, voltaj değişimleri ve içeride bulunan havanın neminin izlenmesi amacıyla anlık bilgilendirme yapabilen sistemler ile takip edilmelidir.
- Sistem odalarının bulunduğu binalarda güvenlik personeli bulunmalı ve tesisin fiziksel güvenliğini sağlamalıdır.
- Sistem odalarında bulunan bütün güvenlik, acil durum ve iklim sistemlerinin periyodik bakımları yapılmalı ve bu bakımlar formlarla takip edilmelidir.
- Sistem odası zemin döşemesi kablo kanallarına ve soğuk hava akışına imkân verecek şekilde uygun bir yükseklikte yapılmalıdır.
- Kullanılacak döşeme malzemeleri kabinlerdeki tam dolu olma durumu göz önünde tutularak 1000 kg kadar basınca dayanabilecek sağlamlıkta seçilmelidir.
- Zemin altında karoları tutan destek ayakları mümkün olduğunca kabin ayaklarının basacağı noktaların altına veya yakınına konarak kabin yüklerinin taşınması kolaylaştırılmalıdır.
- Sistem odaları yangın söndürme sistemlerine sahip olmalıdır.
- Yangın söndürme çözümleri sistem odasında bulunan elektronik cihazlara ve personel sağlığına zarar vermeyecek şekilde olmalıdır. Bu yüzden bu özelliğe sahip gazlar kullanılmalıdır. Yangın söndürmede FM200 kullanılmaktadır.
- Sistem odalarında kullanılan malzemeler yangına dayanıklı olmalıdır.
- Sistem odalarının üzerinden, yanından veya içerisinden hiçbir şekilde aktif su boruları geçmemelidir.

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi



**BİLGİ İŞLEM
DAİRESİ BAŞKANLIĞI**

FİZİKSEL ve ÇEVRESEL GÜVENLİK PROSEDÜRÜ

Doküman No	BGYS-PR19
Yayın Tarihi	06.07.2015
Revizyon Tarihi	16.09.2024
Revizyon No	02
Sayfa No	4 / 5

- Sistem odalarında, sunucu kabinler ve kablolama işleri aşağıdaki standartlar çerçevesinde olmalıdır;
- a. UTP, fiber ve enerji kablolarını birbirinden ayırmak için kanallar kullanılmalıdır. Kablolar birbirinin manyetiğinden etkilenmemelidir. Yanmaz kablolar tercih edilmelidir,
- b. Kablo sonlandırmaları olabildiğince sağlıklı yapılmalı gerekirse sonlandırma yapıldıktan sonra kabloda performans ölçme cihazlarıyla test yapılmalıdır,
- c. Manyetik alanın yüksek olacağı yerlerde mutlaka fiber kablo kullanılmalı, manyetik alandan etkilenmediği için böyle noktalarda veriler fiber ile taşınmalıdır,
- d. Kablolar döşenirken kıvrımlara izin verilmemeli, 90 derecelik keskin dönüşler daha yumuşak şekilde yapılmalıdır. Kabloların kırılmalarını veya dışlarındaki muhafazasına zarar verecek keskin kenarlar üzerinden geçmelerini engelleyecek malzemeler kullanılmalıdır,
- e. Kabinler yerde sabit ayaklarla durmalıdır, küçük sarsıntılarda ileri geri hareket etmelerini engelleyecek bir yapı oluşturulmalıdır. Deprem gibi durumlarda devrilme yer değiştirme gibi ihtimaller düşünülerek yerleşim yapılmalı, kablo bağlantıları çok gergin tutulmamalıdır,
- f. Kabin kapakları mümkünse şifreli olmalı veya kilitli tutulmalıdır ve yetkisiz personel tarafından açılması engellenmelidir,
- g. Gerek elektrik gerek data kablolarında mümkün ise ana bağlantıların yedekli olarak çekilmesine önem verilmelidir. Kabloların yedekliliğinin yanında yedek kabloların sistem odasına mümkün ise farklı bir güzergâhtan girmesi sağlanmalıdır,
- h. Sunucular doğru şekilde etiketlenmeli, sunucu kabinleri çalışma yapılmadığı zamanlarda kilitlenmelidir. Sunucu kabinlerinde kablolamalar düzgün ve kolayca ayırt edilecek şekilde yapılmalıdır. Bütün kablolar ayrı ayrı etiketlenmelidir,
- i. Sunucular arası kablo bağlantıları yer altından yapılmalıdır.
- Sistem odasında bulunan varlıkların sistem odası dışına transferi durumunda, bilgi güvenliği gereksinimleri çerçevesinde gerekli onay ve yetkilendirme işlemleri tamamlanmalıdır, sistem odası dışına transfer edilen varlıklara ait kayıtlar tutulmalıdır.

9. GÜVENLİ ALANLARDA ÇALIŞMA

- Güvenli çalışma alanlarındaki personel veya bu alanda yürütülmekte olan çeşitli faaliyetlerde bulunan personel ve üçüncü parti çalışanları için "ihtiyacı kadar bilme" prensibi uygulanmalıdır.
- Kayıt cihazlarının güvenli alanlara sokulmasına engel olunmalıdır.
- Kullanılmayan güvenli alanlar kilitleniyor ve düzenli olarak kontrol ediliyor olmalıdır.
- Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilmelidir.
- Güvenli bölgelere örneğin sistem odasına yapılan girişler kayıt altına alınmalıdır.
- Bilgi işlem servisleri ile dağıtım ve yükleme alanları ve yetkisiz kişilerin tesislere girebileceği noktalar birbirinden izole edilmiş olmalıdır. Yükleme ve teslimat alanlarından

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi

 BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI	FİZİKSEL ve ÇEVRESEL GÜVENLİK PROSEDÜRÜ	Doküman No	BGYS-PR19
		Yayın Tarihi	06.07.2015
		Revizyon Tarihi	16.09.2024
		Revizyon No	02
		Sayfa No	5 / 5

tesislere yapılacak erişimlerde de BGYS-PL01 Bilgi Güvenliği Politikası 'nda belirtilen hususlar geçerlidir.

10. ZİYARETÇİ KAYITLARININ TUTULMASI

Birimimize gelen ziyaretçiler Gençlik ve Spor Bakanlığı Merkez Binası personel giriş kapısında giriş kaydı yaptırmak zorundadır. Ziyaretçilerin kayıtları burada tutulmaktadır. Ziyaretçi kimlik kartını bırakarak ziyaretçi giriş kartı alır ve bina içerisinde bu kart ile dolaşmak zorundadır. Bu işlemlerin prosedürü Bakanlık Destek Hizmetleri Dairesi Başkanlığı tarafından yürütülmektedir. Giriş kapısından kayıt yaptıran ziyaretçiler birimimiz sekreteryasına kimi ziyaret edeceğini belirtmek zorundadır. Birim sekreterinin ilgili kişiden teyit almasından sonra ziyaretçinin girişine müsaade edilir.

11. UYGUNSUZLUK

Personel görev tanımı formunda tüm BGYS politikaları ve prosedürlerine uygun hareket edeceğini kabul ve taahhüt eder. İhlal durumunda BGYS-PR37 Bilgi Güvenliği ve Disiplin Prosedürü ve mevzuat hükümlerine göre süreç yürütülür.

12. İLGİLİ DOKÜMANLAR

- BGYS-FRM24 FİZİKSEL VE ÇEVRESEL GÜVENLİK DEĞERLENDİRME FORMU
- BGYS-PR37 BİLGİ GÜVENLİĞİ DİSİPLİN PROSEDÜRÜ
- BGYS-LST01 VERİ MERKEZİ GİRİŞ YETKİLİ LİSTESİ
- BGYS-PL01 BİLGİ GÜVENLİĞİ POLİTİKASI

Hazırlayan: BGYS Yönetim Temsilci Yardımcısı	Onaylayan: BGYS Yöneticisi