MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

TEÇHİZAT GÜVENLİĞİ PROSEDÜRÜ

İçindekiler

1 Amaç

Bu doküman, varlıkların kaybedilmesi, hasar görmesi, çalınması veya ele geçirilmesi sonucu kuruluşun faaliyetlerinin kesintiye uğramasını engellemek amacıyla gerekli esasları tanımlar.

2 Kapsam

Bu doküman Bilgi Güvenliği Kapsamı dokümanında belirtilen tüm teçhizatları kapsamaktadır.

3 Sorumluluk

Görev / Rol/Unvan	Dokümanın Hazırlanması	Dokümanın Kontrolü	Dokümanın Onaylanması	Dokümanın Yayınlanması	Dokümanın Güncellenmesi	Dokümanın Uygulanması	Dokümanın Uygulamadan Kaldırılması
Üst Yönetim			X			X	X
Üst Yönetim Temsilcisi			X			X	X
BGYS Yöneticisi	X	X		X	X	X	
BGYS Birim Sorumlusu	X	X				X	
Diğer Çalışanlar						X	

4 Tanımlamalar ve Kısaltmalar

Terim	Tanım/Açıklama
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
BGYS	Bilgi Güvenliği Yönetim Sistemi
Format	Disk biçimlendirme işlemi

5 İşlem Detayı

5.1 Teçhizat Yerleştirme ve Koruma

1. Teçhizat yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine çalışılmalıdır.
2. Kritik veri içeren teçhizatlar yetkisiz kişiler tarafından erişilemeyecek şekilde yerleştirilmelidir.

3. Özel koruma gerektiren teçhizat izole edilmiş olmalıdır.
4. Nem ve sıcaklık gibi parametreler izlenmelidir.
5. Hırsızlık, yangın, duman, patlayıcılar, su, toz, sarsıntı, kimyasallar, elektromanyetik radyasyon, sel gibi potansiyel tehditlerden kaynaklanan riskleri düşürücü kontroller uygulanmalıdır.
6. Bilgi işlem teçhizatlarının bulunduğu lokasyonda veya yakınında sistemleri koruyacak paratoner olmalıdır.
7. Bilgi işlem araçlarının yakınında yeme, içme ve sigara içme gibi faaliyetler yapılmamalıdır.

5.2 Destekleyici Altyapı Hizmetleri

1. Elektrik ve iklimlendirme sistemleri destekledikleri sistem odası için yeterli düzeyde olmalıdır.
2. Elektrik şebekesine yedekli bağlantı, kesintisiz güç kaynağı gibi önlemler ile teçhizatları elektrik arızalarından koruyacak tedbirler alınmış olmalıdır.
3. Yedek jeneratör ve jeneratör için yeterli düzeyde yakıt bulundurulmalıdır.
4. İhtiyaç duyulursa acil durumlarda iletişimin kesilmemesi için servis sağlayıcıdan iki bağımsız hat alınmalıdır.
5. Sunucu odasındaki cihazların (klima, elektrik, ups, vb..) arızası durumunda alarm sistemleri uyarı üretebilecek şekilde konfigüre edilmelidir.

5.3 Kablo Güvenliği

1. Güç ve iletişim kablolarının fiziksel etkilere karşı korunması için önlemler alınmış olmalıdır.
2. Karışmanın ("interference") olmaması için güç kabloları ile iletişim kabloları ayrılmış olmalıdır.
3. Hatalı bağlantıların olmaması için ekipman ve kablolar açıkça etiketlenmiş ve/veya işaretlenmiş olmalıdır.
4. Mümkün olduğunca fiber optik altyapı yapılandırılmalıdır.

5.4 Teçhizat Fiziksel Bakımı

1. Sistem odasındaki teçhizatın (klima, ups, jeneratör) bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde Bilgi İşlem tarafından yaptırılmalıdır.
2. Bakım sadece yetkili personel tarafından yapılıyor olmalıdır.
3. Tüm şüpheli ve mevcut arızalar ve bakım çalışmaları için kayıt tutulmalı ve gözden geçirilmelidir.
4. Teçhizatın bakım için kurum dışına çıkarılırken Teçhizatı Dışarı Çıkartma kurallarına göre kontrolden geçirilmelidir.
5. Teçhizat sigortalıysa, gerekli sigorta şartları sağlanıyor olmalıdır.
6. Üretici garantisi kapsamındaki ürünler için garanti süreleri kayıt altına alınmalı ve takip edilmelidir.
7. Bakım veya arıza giderilmesi ile ilgili yapılan her işlem firmanın hazırlayacağı formlarla kayıt altına alınmalıdır.

5.5 Teçhizatı Dışarı Çıkarma Kuralları

1. Bu esaslar mobil bilgi işlem varlıklarını kapsamamaktadır.
2. Her bir teçhizat için öncelikle yerinde destek hizmeti tercih edilmelidir.
3. Dışarı çıkan teçhizat için üzerinde bulunan uygulamalar ve bilgiler kayıt altına alınır ve geri döndüğünde teslim eden kişi tarafından kontrolü sağlanır.
4. Onarım nedeniyle gönderilecek donanım server, masaüstü ya da dizüstü bilgisayar ise donanım üzerindeki hard disk sökülerek onarıma gönderilir.
5. Kurum dışına çıkacak teçhizat için “Teçhizat Dışarı Çıkarma Formu” düzenlenir. Proje kapsamında kurum dışına çıkartılacak teçhizatlar bu kapsamın dışındadır.
6. Arızalı parça KURUMA ÖZEL veya daha üstü seviyede bilgilerin saklandığı disk ise firma diski yenisi ile değiştirerek arızayı giderir ve eski arızalı disk yükleniciye iade edilmez.
7. Onarım için gönderilen teçhizatlar uygun koruyucu ambalajlama yöntemi ile gönderilmeli, ambalajlar üzerine gereken ikazlar yazılmalı.
8. Bir teçhizatın dışarı çıkarılması esnasında ilgili birimin yönetici onayı alınır.

5.6 Kuruluş Dışındaki Teçhizat ve Varlıkların Güvenliği

1. Kurum alanı dışında bilgi işleme için kullanılacak teçhizat için yetkilendirme yapılıyor olmalıdır.
2. Teçhizatın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyulmalıdır.
3. Evden çalışma ile ilgili tedbirler alınmalıdır. Teçhizatların sigortaları, tesis dışında korumayı da kapsamalıdır.
4. Kurum alanı dışında kullanılacak teçhizatlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanabilecek farklı riskler değerlendirilerek belirlenmelidir.

5.7 Teçhizatı Elden Çıkarma Kuralları

Kullanılmayacak durumda veya ihtiyaç fazlası olan teçhizat "Teçhizat Elden Çıkarma Formu" ile İdari ve Mali İşler Şube Müdürlüğü'ne teslim edilir, elden çıkarma işlemleri "Taşınır Mal Yönetmeliği Genel Tebliği" ne göre yapılır. Teçhizat elden çıkarılacağı veya yedek parça olarak kullanılacağı durumlarda asgari olarak aşağıdaki maddeler uygulanır:

1. Gizli veri bulundurulan teçhizatlar başka sistemlerde yedek parça olarak kullanılmaz ve fiziksel olarak "**Teçhizat Elden Çıkartma Formu**" ile kayıt altına alınarak imha edilir.
2. KURUMA ÖZEL veri bulunduran teçhizatların içindeki veriler tekrar okunmayacak şekilde silindikten sonra ortam kullanılabilir.
3. Tamamıyla imhasına karar verilen her türlü donanım üzerinde bulundurduğu verilere erişim mümkün olduğu durumlarda, yeniden okunmasını engelleyecek şekilde silinmelidir.
4. Kurum içerisinde elden çıkarılacak olan teçhizat öncelikle sınıflandırılarak üzerinde veri olabilecek herhangi bir birim olup olmadığı kontrol edilmelidir. Veri sınıfına göre üst maddeler göz önünde bulundurularak donanımlar sökülerek yedek parça olarak kullanıma alınmalıdır.
5. İmha için dış kurumlar kullanılıyor ise kurumların imha için yetkili olması göz önünde bulundurulur.
6. Tamir ve bakım için gelen cihazların tamiri mümkün değil ise üzerindeki yedek parça olarak kullanılabilecek parçaları, flash bellekleri ve özellikle bilgi bulunan hard diskleri sökülerek "**Teçhizat Elden Çıkartma Formu**" düzenlenerek hurdaya ayrılır.

7. Yedek parça olarak kullanılamayacak durumda olan depolama parçaları fiziksel olarak imha edilmelidir.
8. İmha edilecek cihazlar üzerindeki lisanslı uygulamalar kaldırıldıktan sonra imha işlemleri yapılır.
9. Depolama cihazının içerdiği bilginin bir daha okunamaması için klasik silme veya format işlemlerinin ötesinde yeterli düzeyde işlem yapılmalıdır.
10. Elden çıkarılmak istenen teçhizat aktif cihaz ise (modem, switch, router vb.) default ayarlara getirilerek elden çıkarılır.
11. Eğer kritik bilgi herhangi bir medya üzerindeyse (CD, DVD vb.) ortam kırılarak imha edilebilir.
12. Gizlilik dereceli bilgi içeren, ama geçersizleşmiş, hatalı basılmış, kullanılmayacak olan tüm kâğıtlar, kağıt imha makinası kullanılarak imha edilir.
13. Elden çıkarılan teçhizat mutlaka envanter listesinden düşürülmelidir.
14. İçerisinde bilgi barındırma yeteneği olmayan teçhizatlar zimmet ve envanterden çıkarıldıktan sonra ihtiyaca göre istenildiği gibi kullanılabilir.

5.8 Gözetimsiz Kullanıcı Teçhizatı

1. Başıboş bırakılan bilgisayar ve sunucular 10 dakika içerisinde kilitlenmelidir.
2. Tekrar kullanımı için kullanıcı adı parola ile giriş yapılmalıdır.
3. Mobil cihazlar için "**Mobil Cihaz Kullanım Politikası**" na göre işlem yapılmalıdır.

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					