1. AMAÇ

Bu prosedürün amacı, Erzurum Teknik Üniversitesi bilgi varlıklarının fiziksel tehlikelere ve/veya hasarlara karşı erişilebilirliğini, bütünlüğünü, gizliliğini sağlamak ve bu varlıklar için güvenli bir fiziksel ortam oluşturulmasına yönelik gereksinimleri belirlemektir.

2. KAPSAM

BGYS kapsamında, Erzurum Teknik Üniversitesi tarafından temin edilen, sahip olunan, yararlanılan, bulundurulan ve/veya üretilen bütün bilgi varlıkları bu prosedürün kapsamındadır.

3. TANIMLAR

3.1. BGYS: Bilgi Güvenliği Yönetim Sistemi

3.2. **Varlık:** Şirket bünyesinde kullanılan ve şirket için değeri olan tüm unsurlardır.

4. SORUMLULUKLAR

Bu prosedürün hazırlanmasından ve yönetiminden "Bilgi İşlem Daire Başkanlığı" sorumludur.

5. UYGULAMA

FİZİKSEL ve ÇEVRESEL GÜVENLİK

Kurumsal bilgi varlıklarının fiziksel güvenliğinin sağlanması amacıyla çalışma saatleri içinde ve dışında, Bilgi İşlem Daire Başkanlığı bulunduğu bina giriş çıkışlarını kartlı geçiş sistemiyle kontrol altında tutulur.

5.1. Fiziksel Giriş ile İlgili Genel Kurallar

5.1.1. Bilgi İşlem Daire Başkanlığı

- Bilgi İşlem Daire Başkanlığının bulduğu bina ve katlara yapılan giriş ve çıkışlar, kamera ile izlenir.
- Güvenlik tarafından gelen ziyaretçilerin ziyaret sebebi, ziyaret tarihi ve ziyaretçi bilgileri kayıt altına alınır.

5.2. Ofislerin, Odaların ve Arşivin Güvenliğinin Sağlanması

5.2.1. Giriş Kısıtlamaları

- Personel, Bina ana girişi ve sistem odaları bulunduğu tüm alanlarda kartlı geçiş sistemi ile giriş ve çıkışlar sağlanır.
- Tüm çalışanlar tanımlanmış yetkileri dahilinde giriş çıkış yapabilirler. BT Sistem Odası ilgili bölüm çalışanları ile sınırlı tutulur. Kısıtlama, mümkünse elektronik kart giriş sistemi veya mekanik kilit sistemi ile gerçekleşebilir.
- Kartlı geçiş sistemi erişim yetkilendirmeleri istihdam değişiklikleri ve iş gerekleri doğrultusunda oluşturulan talep ve onaylara istinaden güncellenir.
- Personel giriş kart sistemi iz kaydı (audit log) tutar. Denetim izleri minimum 1 yıl olmak üzere saklanır.

5.2.2. Dış ve Çevresel Tehditlere Karşı Koruma

ISO 27001 standart gereklilikleri ve yasal düzenlemelere uyum sağlamak için ilgili süreçler yürütülür. Dış ve çevresel tehditlere karşı oluşturulmuş Acil Durum Eylem Planları hazırlanır.

5.2.3. Güvenli Alanlarda Çalışma

Tüm ofis alanlarında, bilgi güvenliğini tehlikeye atacak ve risk yaratacak faaliyetlerden kaçınmak esastır ve güvenli alanlarda (sistem odaları vb.), güvenlik kurallarına ek olarak aşağıdaki hususlara dikkat edilir:

- Hizmet sağlayıcılar, BT donanımının veya BT altyapısının bakımı için sistem odasına girdiğinde ya da sistem odasının temizlenmesi sırasında Bilgi İşlem Daire Başkanlığından bir görevli bu kişilere refakat eder ve yapılan işin tümü bu kişi nezaretinde yapılır.
- Sistem odalarında sürekli/uzun süreli çalışma yapılmayacak olup, sadece görevin gerektirdiği sürelerde faaliyette bulunulur.
- Çalışma süresi boyunca, odanın sıcaklık, havalandırma, vb. koşullarını olumsuz yönde etkileyecek faaliyetler gerçekleştirilmez.
- Yiyecek, içecek ile girilmez.
- İşin gerektirdiği cihaz, teçhizat ve kimyasal maddeler dışında herhangi bir malzeme, yanıcı ve/veya parlayıcı kimyasal madde ve risk doğurabilecek benzeri maddeler içeri alınmaz.
- Sistem odaları gibi elektronik aksamın yoğun olduğu odalarda sistemi olumsuz etkileyebilecek kablosuz cihazların (cep telefonu, telsiz telefon, kablosuz bilgisayar vb.) kullanımı izne bağlıdır.
- Cep telefonu kullanımı, fotoğraf ve video çekimine izin verilmez.

5.2.4. Teslimat ve Yükleme Alanları

- Yetkisiz kişilerin ofis alanlarına, depolara ve arşive giriş yapabileceği, teslimat ve yükleme alanları gibi erişim noktaları ve diğer noktalar kontrol edilir ve yetkisiz erişimi engellemek için mümkünse kartlı geçiş sistemi vb. gibi bilgi işleme olanaklarından faydalanılır.
- Ofislere gelen ve giden evrak, kargo vb, ilgili personele teslim edilir.
- Depo alanlarına erişim yetkilendirilmiş personel ile sınırlıdır.
- Gelen malzeme kullanılacağı yere taşınmadan önce, potansiyel tehditlere karşı incelenir.

5.3. Teçhizat

5.3.1. Teçhizat Yerleştirme ve Koruma

- Bilgi varlıkları, çevresel risklerin minimum olduğu bölgelere yerleştirilir.
- Sistem odaları çevresel koşulları kontrol altında olan, dış ve çevresel tehditlere karşı dayanıklı, tüm sunucuların ve ağ cihazlarının kapalı ve kilitli kabinler içinde bulunduğu sadece yetkilendirilmiş personelin girebildiği güvenli alandır.
- İş süreçlerinin sürdürülmesi açısından kritik öneme sahip sunucu ve yerel ağ sistemleri gibi ekipmanlar sıcaklık, rutubet, havalandırma, fiziksel erişim ve benzeri şartların kontrol edildiği sunucu odasında saklanır. Kritik manyetik medyalar, diskler, depolama cihazları kilitli bir ortamda muhafaza edilir.
- Sistem odalarına girişler ve çıkışlar kartlı sistemi ile gerçekleştirilir. Giriş ve çıkışlara ait denetim izleri en az bir sene boyunca saklanır.
- Sistem odalarının iklimi mümkünse yedekli klima sistemi ile kontrol altına alınır, gerekli görülen sistem odaları için yangın söndürme sistemi kullanılır. Tüm sistem odalarında yangın söndürme tüpü bulunur. Sistem odalarının nem ve sıcaklığı sürekli olarak izlenir ve kayıt altında tutulur.
- Sistem odalarının erişim yetkileri yılda bir gözden geçirilir.

5.3.2. Ağ Dağıtıcılarının (Hub & Switch) Fiziksel Güvenliği

- Ofislerde bulunan ağ dağıtıcıları yetkisiz erişimden korunması amacıyla kilitli kabinlerde tutulur ve kabinetler ısı, toz ve sudan korunacak şekilde yerleştirilir.

- Tüm ağ girişlerine (network jacks) ve erişim noktaları sadece yetkili çalışanlar tarafından erişilebilir durumda muhafaza edilir.
- Bilgi İşlem Daire Başkanlığı personeli, ağ dağıtıcı cihazların fiziksel güvenliğinin sağlanması için gerekli önlemleri almak ile sorumludur.

5.3.3. Destekleyici altyapı hizmetleri

Destekleyici altyapı hizmetleri kurumun iş sürekliliği açısından kritiktir. Altyapı düzenlemeleri şu şekilde yapılır:

Yerel Güç Kaynağı

Sistem odaları içerisinde kullanılan gerilim, sunucuların kılavuzlarında belirtilen değerlere uygun olacak şekilde düzenlenir. Donanımın hat gerilimindeki aşırı artıştan korunması için uygun kapasiteli güç kesiciler kullanılır.

Kesintisiz Güç Kaynağı (UPS)

Bilgi İşlem Daire Başkanlığı dahilinde PC ve çevre birimlerine destek veren ve birbirini destekler şekilde çalışan UPS'ler bulunur. UPS'ler havalandırma açısından ideal olan ve kilitli kapı ile muhafaza edilen bir ortamda bulundurulur. UPS'ler doğru çalıştığının kontrol edilmesi amacıyla düzenli olarak test edilir.

Jeneratör

Jeneratörler kampüs yönetimi tarafından yerel güç kaynağı kesildiğinde sorumlu bakım personeli tarafından ya da otomatik olarak devreye girecek şekilde konfigüre edilir. Jenaratörler düzenli aralıklara doğru çalıştıklarına dair test edilir.

Sıcaklık ve Hava Kirliliği

BT donanımlarını etkileyebilecek tozun, ısının ve hava kirliliğinin kontrol altında tutulması için klimalar kullanılır. Klimalar yedekli yapıda kurulur. Klimaların bakımının düzenli olarak yapılması sağlanır.

Sıcaklık ve nem ölçen cihazların gerektiğinde kalibrasyonu yapılır, alarmların minimum ve maksimum değerleri incelenir. Güvenli bölgelerdeki iklim şartları sürekli olarak izlenir.

Sistem odalarında, sıcaklığın 20 ila 30 derece seviyesinde tutacak uygun özellikte ve sayıda klima bulundurulur.

Sistem odasının periyodik temizliği, sistem odası sorumlularının refakati dâhilinde gerçekleştirilir.

Yangın Güvenliği

Sistem odalarının tümü yangın algılama sistemi ile desteklenir ve yangın söndürme sistemi olarak FM200 veya yangın tüpleri ile donatılır. Yangın Söndürme, yangın algılama ve yangın tüplerinin periyodik bakımları yapılır.

Yıldırım Güvenliği

Uygun yüksek noktalara (Bina çatıları, Su kuleleri, anten direkleri vb.) paratoner yerleştirilir.

Su Hasarı Güvenliği

Selden korunma: Binalar ve arşiv uygun su tahliye kanallarına sahiptir. Tesislerin su sızıntısına karşı bakımı yaptırılır ve sızıntının tespit edilmesi durumunda bakım onarım ekibi tarafından uygun önlemler alınır.

Su Tahliye Sistemi: Su tahliye sistemi, suyun ve su tahliye boruları, sistem odalarından uzak olacak şekilde konumlandırılır.

Sistem odasında su sızıntısı vb. durumlar için zeminde su sensörleri kullanılır.

Diğer

Yüksek öneme sahip sistem odalarında aşağıdaki maddeler bulunur:

- Kabinetler tabanı yükseltilmiş olup, kat seviyesinden 10 cm yüksektir.
- Tavan aydınlatma, duman, yangın algılama sistem donanımlarının uygun şekilde yerleştirilmiştir.
- Kapı girişleri, kimlik kartı okuma, parmak izi okuma veya parola sistemleri ile kontrol edilmektedir. Bu sistemlerin enerjileri kesintisiz güç kaynağından sağlanarak kesintisiz enerji sürekliliği sağlanmıştır.
- Prizler topraklanır ve hatalı kablolama veya kısa devreye karşı güç kesicilerle desteklenir.

5.3.4. Kablo Güvenliği

Güç ve veri taşıyan veya bilgi teknolojilerini destekleyen haberleşme kabloları hasar veya dinlenmeye karşı korunur. Şu hususlar göz önünde bulundurulur:

- BT sistemleri ve destek sistemlerine ilişkin enerji, veri bağlantısı ve benzeri kablolar fiziksel etkilere ve yetkisiz erişimlere karşı korunmalıdır. Bu bağlamda, söz konusu kabloların mümkün olan en iyi şekilde korumaya alınması ve erişilmesi zor bir şekilde yerleştirilmesi gerekir. Binalara ve sistem odalarına giren güç ve haberleşme hatları üst taraftan geçirilir veya uygun biçimde korunur.
- Ağ pasif elementleri, yetkisiz müdahaleye veya hasara karşı kablo kanalları/boruları kullanılarak korunur.
- Veri kabloları ile güç kabloları birbirlerinden mümkün olduğunca ayrı tutulur, birbirlerine yakınlıkları sebebiyle oluşabilecek olumsuz etkiler önlenir.
- Herhangi bir kabloda meydana gelebilecek hasarlar veya arızalar sebebiyle oluşabilecek hizmet kesintilerini önlemek amacıyla, mümkün ise alternatif/yedek kablolar kurulur ya da bulundurulur.
- Kabloların bağlandığı paneller ve odalara erişim kartlı kontrol sistemleri ve/veya kilit sistemleri ile gerçekleştirilir.
- Kablolar yetkisiz erişime karşı koruma altına alınır. Yetkisi olmayan çalışanların kablolama faaliyetlerini yürütmesi yasaktır.

5.3.5. Teçhizat (Elektronik Ofis Donanımları) Bakımı

Bilgi İşlem Daire Başkanlığı sunucuların yönetiminden sorumludur.

- Bakımlar üretici firmaların tavsiyeleri doğrultusunda, uygun zamanlarda ve doğru şekilde yapılır. Bu bağlamda, her bir cihaz için uygun bakım takvimleri hazırlanır ve takip edilir.
- Bakımlar sadece yetkili servis ve/veya yetkili personel tarafından, ilgili talimatlara uygun olarak gerçekleştirilir, kullanıcıların ve yetkisiz kişilerin cihazlara müdahalesine izin verilmez.
- Şüphelenilen veya karşılaşılan tüm hataların, önleyici ve düzeltici bakım işlemlerinin kayıtları tutulur.
- Bakım zamanı belirlendiğinde, bu bakım işleminin kuruluş çalışanları ya da üçüncü taraflar tarafından yapılıp yapılmayacağına göre uygun kontroller gerçekleştirilir; mümkün olduğu durumlarda, kritik bilgi donanımlardan temizlenmeli veya servis personeli tarafından gerektiği şekilde temizlenir.
- Yapılan bakımlar tarih ve kontrol ayrıntılarını içerecek şekilde kayıt altına alınır.
- Sigorta poliçelerinin zorunlu tuttuğu tüm gereksinimlere uyulur.
- Bakım ve/veya onarım için kurum dışına çıkarılması gereken ve bilgi depolama özelliğine sahip cihazlar (bilgisayarlar, cep telefonları vb.) kurum dışına çıkarılmadan önce incelenerek, içlerindeki hassas bilgiler geri getirilemeyecek yöntemler ile silinir.

5.3.6. Önleyici Bakım

Önleyici bakım, sunucu ve ağ donanımlarına kesintisiz erişilebilirlik için gerekli olan, BT donanımları üzerinde gerçekleştirilen önemli bir işlemdir. Tipik bakım faaliyetleri şunlardan oluşur:

- Sabit disk kapasitesinin kontrol edilmesi ve disk yüzeylerinin bozuk sektörlere yönelik taranması,
- Geçici dosyaların ve yedeklenen denetim izi dosyalarının temizlenmesi,
- Düzenli temizliğin sürdürülmesi (tozdan arındırma, döküntü ve kirliliğin ortadan kaldırılması vs.) ve kablolama bütünlüğünün düzenli kontrol edilmesi (kablo sonlarının eklentileri, fazla kablo uzantılarının sarılması, düzenli kablo yolları, temiz kablo bağlantıları)
- Batarya tertibatının bakımı, güç kablolarının bağlantılarının düzgünlüğü, topraklama uçlarının ve kablo yollarının düzgünlüğü ve bütünlüğü, muhafaza şasisinin bütünlüğünü içeren UPS Güvenliği vs.
- Vida ve cıvataların sıkılığı, donanımın bir yerden bir yere kaydırılması anındaki dikkat ve buradaki yardımcı bağlantıların kontrolünü içeren fiziksel kurulum bütünlüğü
- Bakım faaliyetleri, donanım ve hizmeti sağlayan kişilere göre farklılık gösterebilir. Sistem yöneticileri ve ağ yöneticileri tüm BT donanımının bakım gereksinimlerini belirler ve önleyici bakım programını belirler.
- Satın alma anlaşmasının bir parçası olarak bir kısım donanım için, satıcılar önleyici bakımları sağlar. Bu bakım programı bakımlara ilişkin programa eklenir.
- Sistem ve ağ yöneticileri hazırlanan önleyici bakım programına göre bakımları gerçekleştirirler.
- BT Sorumlusu bakım hizmetini sağlayan tarafların bakım programına uyduğunu kontrol eder.

Tüm bakım faaliyetleri için yöneticiler:

- Önleyici bakım programının ve bu kapsamdaki faaliyetlerin kritik veya hassas uygulamaları aksatmamasını ve herhangi bir şekilde etkilememesini,
- Bakım faaliyetlerinin verinin yoğun olarak işlendiği kritik dönemler ve yedekleme veya geri yükleme gibi diğer BT faaliyetleri ile çakışmamasını,
- Tüm taraflara herhangi bir bakım faaliyeti öncesinde bilgi vermesi işlemlerini gerçekleştirir.

5.3.7. Varlıkların Taşınması

Bakım amacı ile 3. taraf firmaya gönderilmesi gereken bilgi içeren varlıklarının yedeği alınır ve üzerindeki veriler güvenli silme yöntemleri ile temizlenir. Bilgi teknolojileri teçhizatının bakım amacıyla, BT sorumlusunun izni olmadan kuruluş dışına çıkarılması yasaktır. Bilgi İşlem Daire Başkanlığı personelinin kullandığı dizüstü bilgisayarlar ve telefonlar kuruluş dışına çıkartılabilir. Bu noktada kuruluş dışına çıkarılan bilgisayarların ve telefonların güvenliğinden personel kendisi sorumludur.

5.3.8. Teçhizatın Güvenli Yok Edilmesi veya Tekrar Kullanımı

Saklama ortamları, kullanımına ihtiyaç olmadığında güvenli ve tehlikesiz şekilde imha edilir. Saklama ortamları yeterli özen gösterilmeden imha edildiğinde, hassas bilgi başka kişilerin eline geçebilir. Riski en aza indirmek amacıyla veri depolama ortamlarının güvenli imhası için resmi prosedürler takip edilir. Veri depolama ortamlarının imhasında aşağıdaki esaslar değerlendirilir.

- Hassas bilgi ve lisanslı yazılım içeren saklama ortamları güvenli ve tehlike içermeyecek şekilde saklanır ve imha edilir (yakarak, parçalara ayırarak, kuruluş içerisinde başka bir uygulama tarafından kullanılmadan önce format atılarak, anlaşma kurumlar aracılığı ile vb.).
- Aşağıdaki liste güvenli imhası gereken malzemeleri listelemektedir:
  - Kâğıt dokümanlar;
  - Ses veya diğer kayıtlar;
  - Çıktı raporları;
  - Manyetik kasetler;
  - Çıkarılabilir disk ve kasetler;
  - Optik depolama ortamları (tüm formlar ve yazılım dağıtıcı ortamlar da dâhil);
  - Program dökümü;
  - Test verisi;
  - Sistem dokümantasyonu.
- Hassas malzemelerin imhasına yönelik denetim izi tutulur.
- İmha için malzeme toplanması sırasında, gizli olarak nitelendirilmeyen bilginin miktarı artarak bir grup gizli bilgiden daha hassas ve daha kritik bir hale dönüşebilir. Bu yığın etkisine özel olarak dikkat edilmektedir.

BT bilgi varlıklarının imha süreci ile ilgili detaylar PR.17 İmha Prosedürü içinde tanımlanmıştır.

5.4. Ek Kontroller

5.4.1. Yiyecek, İçecek ve Sigara Kullanımına İlişkin Kısıtlamalar

İçinde bilgi varlıklarının bulunmadığı özel olarak belirlenmiş (bina dışındaki sigara içmeye mahsus alanlar gibi) alanlar dışında Bilgi İşlem Daire Başkanlığı ofislerinde sigara içilmesi yasaktır. Bilgi varlıklarına yakın mesafede yemek yenilmesi ve bir şeyler içilmesi tavsiye edilmez, yenecekse de çok dikkatli olunmalıdır. Sistem odasında yiyecek, içecek tüketmek ve sigara içmek yasaktır.

5.4.2. Çöp

Çöpler uygun kaplarda ve periyodik olarak toplanır. Çeşitli bilgi içeren varlıklar çöpe atılmadan veya bilgi sisteminden çıkartılmadan önce, varlıklarda yer alan kayıtlı bilgiler yedeklenir ve atılacak olan varlıktan silinir. Çöpe atılacak olan evraklar kırpılmadan çöpe gönderilmez.

5.4.3. Sıvıların ve Yanıcı Maddelerin Saklanması

Sıvılar, temizlik maddeleri ve diğer sıvılar kapalı kaplarda ve bilgi varlıklarından uzakta muhafaza edilir. Yanıcı maddeler, bilgi varlıklarından uzakta emniyetli ve güvenli bir şekilde muhafaza edilir.

6. İLGİLİ DOKÜMANLAR

-

	HAZIRLAYAN	ONAYLAYAN
ÜNVANI	BGYS YÖNETİM TEMSİLCİSİ (DAİRE BAŞKANI)	GENEL SEKRETER
ADI SOYADI	Dr. Naci BAYRAK	Prof.Dr. Ahmet DUMLU
İMZA		