AMAÇ

Bu politika Kurumun "Veri Merkezi ve Sistem Odalarının" standartları ve güvenliğinin sağlanması için gerekli minimum koşulları belirlemek amacıyla hazırlanmıştır.

KAPSAM

Bu politika Konya Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı'nın hizmet vermesi için gerekli olan tüm uygulama ve donanımları, fiziksel altyapıyı, bu sistemlerin içinde bulunduğu ortamı ve konuyla ilgili sorumluları kapsar.

DAYANAK

Bu politikanın temel dayanağı TS ISO/IEC ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YÖNERGESİ ve ilgili diğer mevzuattır.

SORUMLULAR

Bu politikanın uygulanmasından Bilgi İşlem Daire Başkanı, Sistem ve Ağ Birimleri ile Bilgi İşlem Daire Başkanının sistem odasına giriş yetkisi verdiği personel sorumludur.

KURALLAR

1. SİBER GÜVENLİK İÇİN ALINACAK ÖNLEMLER

1.1. Sunucular sistem odasında tutulacaktır.

1.2. Sunuculara, kullanım amacına yönelik olarak işletim sistemi ve diğer yazılımlar kurulmalıdır. Gereksiz yazılım ya da bileşenleri kaldırılmalıdır.

1.3. Sunucu üzerinde çalışan işletim sistemlerinin, sistem yazılımlarının ve güvenlik amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Antivirüs ve sunucu güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.

1.4. Değişim Yönetimi Politikaları sunucular için de uygulanacaktır.

1.5. Sunucu günlükleri düzenli aralıklarla denetim ve izlemeye tabi tutulacaktır.

1.6. Sunucuların uzaktan yönetimi gerekiyor ise; yönetim konsolu ve sunucu arasındaki haberleşme güvenli kanal ve tekniklerle gerçekleştirilecektir.

1.7. Sunuculara kurum dışından yapılması gerekli bağlantılar için, bağlanacak kişi ve kurumla gizlilik sözleşmesi yapılmalıdır.

1.8. Sunuculara kurum dışından yapılacak bağlantılar için noktadan noktaya bağlantı kurulması sağlanmalıdır. Bağlantı yapacak dış kaynağın sabit IP adresi olması gereklidir.

1.9. Sunucular dış kaynaklara açılacak ise; bağlantı yapılması gereken servis ve portlar dışındaki (örn. http/https/sftp, 80/443,22 vb.) diğer portlar güvenlik cihazı (firewall vb.) seviyesinden başlamak üzere iletişime kapatılmalıdır.

2. FİZİKSEL ERİŞİM İÇİN ALINACAK ÖNLEMLER

a) Sistem odaları yetkisiz personelin bilerek veya kaza ile erişiminin engellenmesi amacıyla her zaman kilitli tutulmalıdır

b) Sistem odalarının bulunduğu binaların girişlerinde 24 saat güvenlik görevlisi bulundurulmalıdır.

c) Sistem odalarının bulunduğu binalara girişte ziyaretçilerin kaydı (kimi ziyaret ettikleri, giriş ve çıkış saatleri) alınıp imzaları ziyaretçi kayıt defterinde tutulmalıdır.
d) Elektronik giriş kartları veya biyometrik yöntemlerle sistem odalarına erişim sadece düzenli olarak kullanması gereken personel ile sınırlandırılmalıdır.
e) Sistem odasına girmeye yetkili olmayan ama bakım, onarım ve altyapı çalışmaları gibi sebeplerle odaya girmesi gereken kurum/firma çalışanları odaya giriş yetkisi olan Bilgi İşlem Daire Başkanlığı personeli nezaretinde odada çalışmalıdır. Bu kişiler için ayrıca "Bilgi İşlem Sistem Odası Ziyaretçi Defteri" doldurulur ve imzalatılır.

3. ÇEVRESEL GÜVENLİK İÇİN ALINACAK ÖNLEMLER

3.1. Oluşabilecek problemlere karşı sistem odaları kontrol yazılımı ve sensörleri içeren donanım kullanılmalıdır.
3.2. Sistem odalarının bulunduğu binaların çatı, su ve kanalizasyon borularının düzenli bakımı, ilgili birimle resmi yazışma yapılarak sağlanır.
3.3. Duman dedektörü ve yangın alarmı konumlandırılmalıdır.
3.4. Yangın söndürme sistemi bulunmalıdır. Sistem odasına erişim hakkı verilen personele yangınla mücadele konusunda eğitimler verilmelidir.
3.5. Su baskınına karşı yerden yükseltilmiş taban kullanılmalıdır.
3.6. Kabinet ve cihazlarda depreme karşı sabitleme yapılmalıdır
3.7. Sistem odaları elektrik kesinti ve arızalarına karşı kesintisiz güç kaynağı (UPS) ve jeneratör ile desteklenmelidir.
3.8. Sistem odalarında ısı ve nem farklılıklarının önüne geçebilmek amacıyla iklimlendirme sistemleri kullanılmalıdır.
3.9. Sistem odalarında meydana gelebilecek olağanüstü durumlarda sorumlu kişileri bilgilendirecek uyarı sistemleri (sms, e-posta, telefon ile aranması gibi) oluşturulmalıdır.
3.10. Sistem odaları dikkat çekmeyecek şekilde konumlandırılmalıdır. Sistem odalarını açık bir şekilde belirten tabela vb. yazılardan kaçınılmalıdır.
3.11. Sistem odası yerleşim düzeni, kablolama altyapısı ve kablo kanalları dokümante edilmelidir.
3.12. Sistem odalarında her türlü yeme, içme yasaklanmıştır.
3.13. Sistem odasının ve donanımların sürekli temiz ve düzenli olmaları sağlanmalıdır.
3.14. Sistem odasında karton, kâğıt vb. diğer kolay yanabilen türde malzemeler bulundurulmaz.
3.15. Sistem odası, depolama amaçlarıyla kullanılamaz.
3.16. Sistem odası erişim yetkileri, en çok 6 aylık periyotlarla birim yöneticisi tarafından kontrol edilir.
3.17. Sistem odası,7/24 süreyle kameralar aracılığıyla gözlenir. Kamera kayıtları, herhangi bir uygunsuzluğun araştırılabilmesi amacıyla yeteri kadar süreyle saklanır.
3.18. Sistem odasında bulunan tüm malzemelerin envanter kaydı yapılır.
3.19. Sistem odasında çalışacakların ve 3. Tarafların güvenliği ve sağlığına ilişkin 6331 Sayılı İş Sağlığı ve Güvenliği Kanunu hükümlerine uygun kontroller uygulanır.
3.20. Sistem odasında sesli ve görüntülü kayıt yapılmasına izin verilmez.

4. BAKIM

4.1. Sistem Odalarının bakımı sadece yetkili personel tarafından yapılmalıdır.

4.2. Cihazların bakımı üreticinin tavsiye ettiği zaman aralığında yapılmalıdır.
4.3. Kullanıcıların işlerini aksatmamak için sunucuların bakımı mesai saatleri dışında yapılmalıdır.
4.4. Bakım yapılmadan önce kesintiden etkilenecek birimlere haber verilmelidir.
4.5. Bakıma başlandığında cihazın enerjisi kesilmelidir.
4.6. Sunucular garanti altında ise, garanti şartları neticesinde bakım sağlanmalıdır.
4.7. Sunucular herhangi arızadan dolayı kurum dışına çıkarılacaksa seri numarası, marka modeli belirtilerek teslim tutanağı hazırlanmalıdır.

YÜRÜRLÜK

1- Bu politika, BGYS komisyonu tarafından onaylandıktan sonra Bilgi İşlem Daire Başkanlığının web sayfasında yayımlanarak duyurusu yapıldığı tarihte yürürlüğe girer.

YÜRÜTME

1- Bu politika, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.