# AMAÇ:

# Üniversitemizdeki sunucu sistemlerinin sürekli olarak doğru bir şekilde çalışmasını sağlamak ve sistemlerin güvenliğini sağlamak için gerekli yönergeleri sağlamaktır. Bu talimatlar, sunucu bina veya odalarının herhangi bir arıza, bozulma veya veri kaybı riski olmadan verimli bir şekilde çalışmasını sağlamak için oluşturulmuştur. Bu talimatın amacı üniversitenin tüm iletişim türlerinde bilgi transferinin güvenli yöntemlerle yapılmasını sağlamak için kuralların tanımlanmasıdır.

# KAPSAM: Bilgi Güvenliği kapsamında yürütülen tüm birimleri kapsamaktadır.

1. **SORUMLULUK**:

Binaların Sunucu odasının kontrol ve bakımından sorumlu personeller, birim amiri veya atanan kişilerdir. Kontrol ve bakım hizmetleri, gerektiğinde uygun hizmet şirketleri tarafından da yürütülebilir. Sunucu odası raporlamasından da sorumludurlar.

1. **TEKNİK** **TERİMLER**

* BİDB – Bilgi İşlem Daire Başkanlığı

1. **UYGULAMA**

Sorumlu personel, ilgili birimin yöneticisi tarafından teknik olarak uygun koşulları sağlayan personeller arasından seçilir ve seçilmiş olan personel Sunucu Odası Raporu ile BİDB'ye bildirilir. Eğer sorumlu personel seçilmemişse, birim yöneticisi sorumludur. Her yıl BGYS kalite iç denetimlerinden önce birim tarafından FR-1857 – Sunucu Odası Denetim Raporu istenilir.

Sistem odasında aşağıdaki konu başlıklarına dikkat edilmeli ve uygulanmalıdır:

* + Sunucu odası bulunan birim, Sivil Savunma, İş güvenliği koord, Bakım Onarım, BİDB Ağ ve Sistem şube Müdürlüğü destek almalıdır.
  + Üniversite içi kaynaklardan (Destek birimi vb.) veya dışarıdan teminle yapılan tüm işlemleri rapor ve çizelgeler halinde dosyalayıp takip etmekle sorumludur.
  + Bakım anlaşmaları ve çizelgelerini birim veya sorumlu personel istenildiği anda sunmak zorundadır.
    1. Yangın Sistemi: Sunucu odalarında yangın çıkması durumunda yangının erken tespit edilmesi ve müdahale edilmesi için kurulan sistemdir. Yangın algılama ve söndürme sistemleri, duman dedektörleri, yangın söndürme tüpleri gibi elemanları içerir. Yangınlar için Sivil savunma talimatları dikkatte alınmalıdır.
    2. Yedekleme Sistemi: Sunucu odalarında saklanan verilerin kaybolmaması için kullanılan sistemdir. Yedekleme sistemleri, verilerin periyodik olarak başka bir depolama ortamına kopyalanmasını sağlar.Yedekleme planı kurtarma senaryoları ve Veri imhanın YD-080 İmha politikasına göre yapılması gerekmektedir.
    3. Klima Sistemi: Sunucu odalarının sıcaklık ve nem seviyelerini kontrol altında tutmak için kullanılan sistemdir. Sunucuların çalışma sıcaklıklarını ve nem seviyelerini belirli aralıklarla ölçen sensörlerle birlikte kullanılır.
    4. UPS Sistemi: Sunucuların kesintisiz güç alabilmesi için kullanılan sistemdir. Kesintisiz güç kaynağı olarak da bilinir. Elektrik kesintilerinde sunucuların çalışmasını sürdürmesine olanak tanır.
    5. Sıcaklık Sensörü: Sunucu odasının sıcaklığını ölçen cihazdır. Sıcaklığın belirli bir aralıkta tutulması, sunucuların sağlıklı çalışmasını sağlar. önerilen sıcaklık aralığı 18°C - 27°C arasındadır.
    6. Nem Sensörü: Sunucu odasının nem seviyesini ölçen cihazdır. Nem seviyesinin belirli bir aralıkta tutulması, sunucuların sağlıklı çalışmasını sağlar. Nem seviyesi genellikle %40 ile %60 arasında olması önerilir.
    7. Elektrik Panosu: Sunucu odasındaki tüm elektrik sistemlerinin ana kontrol noktasıdır. Elektrik panosunda enerji kaynağı, kesiciler, sigortalar, voltaj ve akım ölçüm cihazları gibi elemanlar bulunur. Elektrik pano önlerinde yalıtım paspasları bulunmalıdır.
    8. Jeneratör: Elektrik kesintilerinde enerji sağlayan bir güç kaynağıdır. Jeneratörler, sunucuların kesintisiz çalışmasını sağlar ve yedekleme sistemi ile birlikte kullanıldığında verilerin kaybolmasını önler.
    9. Havalandırma: Sunucu odalarında sıcak havanın dışarı atılması ve taze hava akışı için yeterli miktarda havalandırma sistemi bulunmalıdır.
    10. Güvenlik: Sunucu bina veya odalarının kapıları, girişleri ve pencereleri kilitli tutulmalı. Anahtar sadece yetkili personelde olmalı , izinsiz erişimler için güvenlik ihlalleri rapor edilmeli ve anahtarın değiştirilmesi gerekmektedir.
    11. Harici bir uygulama varsa (yangın söndürme otomasyonu vb) denetim raporuna işlenmelidir.
    12. Denetim Raporuna sunucu odasında bulunan cihazlar aşağıdaki örneğe benzer şekilde listelenmelidir.
    13. Kayıt tutma: Bakım ve onarım faaliyetleri, bir kayıt tutma sistemine kaydedilmelidir. Bu kayıtlar, hangi faaliyetlerin yapıldığını, hangi ekipmanların değiştirildiğini ve ne zaman yapıldığını belgelemek için kullanılabilir. Bu bilgiler, sunucu odasındaki ekipmanların bakımı ve onarımı için gereken planlama ve bütçeleme süreçlerinde de yararlı olabilir.
    14. Erişim Yetkileri : Sunucu , oda ve verilere erişimlerin listelenmesi ve kontrol edilmesi.

# DAĞITIM ve RAPORLAMA :

Tüm Birim yöneticilerine bilgilendirme yapılması ve FR-1857 formunun her yıl ISO 27001 iç denetimler öncesi BİDB ağ ve sistem şube müdürlüğü tarafından istenir ve toplanır. Toplanan raporlar BGYS ekibi tarafından değerlendirilir ve raporlanarak ilgili veri oda sorumlularına Ağ ve Sistem şube müdürlüğü tarafından bilrdirilip takibi yapılır.

1. İlgili Dökümanlar:
   * FR-1857 – Sunucu Odası Denetim Raporu
   * YD-084-Yedekleme ve Yedekten Geri Dönme Politikası
   * PR-038-Varlık Yönetimi Prosedürü
   * PR-026-Kriptografik Kontroller Prosedürü
   * YD-079-Erişim Politikası
   * PR-043-Kurumsal Erişim ve Yetkilendirme Prosedürü