1. **AMAÇ:** Bilgi yönetim sistemine yönelik yazılım donanım ile ilgili sorunlar, bilgi güvenliği bilgi mahremiyeti gibi konularda risk değerlerini belirlemek, meydana gelebilecek sorunlar ve bu sorunlara çözüm bulmak ve kontrolünü sağlamak.
2. **KAPSAM:** Tüm birimleri ve tüm birim çalışanlarını kapsar.
3. **SORUMLULAR:** Dekan, Dekan Yardımcısı, Fakülte Sekreteri,
4. **KISALTMALAR**
5. **TANIMLAR**
6. **FAALİYET AKIŞI**

Risk Analizi

Harici Tehdit Unsurları:

- Bir saldırganın kurum web sitesini değiştirmesi
- Bir saldırganın kurumun korunan bilgisini çalması
- Birçok saldırganın kurum web sunucusunu servis dışı bırakma saldırısı yapması

Dahili Tehdit Unsurları:

- Bilgisiz ve bilinçsiz kullanım
  - Temizlik görevlisinin sunucunun fişini çekmesi
  - Eğitilmemiş personelin veri tabanını silmesi
- Kötü niyetli hareketler
  - İşten çıkarılan çalışanın kuruma ait web sitesini değiştirmesi
- Genel güvenlik olayları
  - Türkiye'de kamu kurumuna yönelik saldırılar

Şifre Güvenliği:

- Hiç kimse ile herhangi bir şekilde paylaşılmamalıdır.
- Mümkünse bir yere yazılmamalıdır. Yazılması gerekiyorsa güvenle bir yerde muhafaza edilmelidir.
- Güvenli olmadığını düşündüğünüz mekanlarda kurumsal şifrelerinizi kullanmanızı gerektirecek uygulamaları kullanmayınız.
- Bilgi yönetim sisteminde HBYS üzerinden şifre verildikten sonra sistem güvenliği için kişinin şifresini yenilemesi gerekir.

Yazılım Yükleme-Güncelleme:

- Kurum tarafından belirlenmiş yazılımların dışında bilgisayarlarda program bulunmamalıdır.
- Güvenilir olmayan sitelerden yazılımlar indirilmemeli ve yazılımlar kullanılmamalıdır.

Donanım Ekleme:

-Bilgisayarlara modem takılmamalıdır.
- Bluetooth ve 3G modemlerle internet bağlantısı yapılmamalıdır.

Zaralı Donanımlar, Virüsler:

- Tüm bilgisayarlarda virüs koruma programı çalıştırılmalı ve güncellemesi yapılmalıdır.
- Antivirüs programı kapatılmamalıdır.
- Dosyalar virüs taramasından geçirilmelidir.

Risk İzleme Planı:

Aşağıdaki tablo BT sistemlerinde sıklıkla karşılaşılan tehditleri ve bunların kaynaklarını içermektedir (tehdidin kaynağı bölümünde kullanılan kısaltmalar B: İnsan kaynaklı ve bilerek, K: İnsan kaynaklı ve kazayla, D: Doğal, Ç:Çevresel).

Tehdit	Tehdidin Kaynağı
Deprem	D
Sel	D
Fırtına	D
Yıldırım	D
Endüstriyel bilgi sızması	B,K
Bombalama ve silahlı saldırı	B
Deprem	D
Güç kesintisi	B,K,Ç
Su kesintisi	B,K,Ç
Havalandırma sisteminin arızalanması	B,K,Ç
Donanım arızaları	K
Güç dalgalanmaları	K,Ç
Tozlanma	Ç
Elektrostatik boşalma	Ç
Hırsızlık	B
Saklama ortamlarının izinsiz kullanılması	B,K
Saklama ortamlarının eskiyip kullanılmaz duruma	K
Personel hataları	K
Bakım hataları/eksiklikleri	K
Yazılımların yetkisiz kullanılması	B,K
Kullanıcı kimlik bilgilerinin çalınması	B,K
Zararlı yazılımlar	B,K
Yetkisiz kişilerin ağa erişimi	B
Ağ cihazlarının arızalanması	K
Hat kapasitelerinin yetersiz kalması	B,K
Ağ trafiğinin dinlenmesi	B
İletim hatlarının hasar görmesi	B,K

Mesajların yanlış yönlendirilmesi	K
Mesajların yetkisiz kişilere yönlendirilmesi	B
İnkar etme	B
Kaynakların yanlış kullanımı	K
Kullanıcı hataları	K
Personel yetersizliği	K

Risk Değerlendirilmesi (Analiz):

- Riskin büyüklüğünü tahmin etmek ve riske tahammül edilip edilemeyeceğine karar vermek, tehlikelerin sonucunda oluşabilecek risklerin giderilmesinde öncelik sırasının oluşturulması için kullanılan yöntemdir.

- Değerlendirme yapılırken tehlikeler, 5 x 5 matematiksel risk yöntemine göre yapılır. Risklerin puanlanmasında aşağıda verilen tablodaki olasılık ve şiddet değerleri kullanılır. Risk analizi yapılırken risklerin en kötü durumu göz önünde bulundurulur.

- Risk Derecesi: Yapılan analiz neticesinde risk derecesi, riskin gerçekleşme olasılığı (İhtimali) ile şiddetinin sayısal değerinin çarpımı ile bulunur. **Örnek: Risk Derecesi (Puanı) = Olasılık X Şiddet (RD= O x Ş)**

4.7. İhtimal/Olabilirlik skalası

İşletme şartlarında bir olayın gerçekleşme ihtimalini göstermek için aşağıdaki ihtimal skalası kullanılır;

İHTİMAL	ORTAYA ÇIKMA OLASILIĞI İÇİN DERECELENDİRME BASAMAKLARI	SKOR
ÇOK KÜÇÜK	HEMEN HEMEN HİÇ	1
KÜÇÜK	ÇOK AZ (YILDA BİR KEZ) SADECE ANORMAL DURUMLARDA	2
ORTA	AZ (YILDA BİRKAÇ KEZ)	3
YÜKSEK	SIKLIKLA (AYDA BİR)	4
ÇOK YÜKSEK	ÇOK SIKLIKLA (HAFTADA BİR,HER	5

GÜN, NORMAL ÇALIŞMA ŞARTLARINDA)