1. AMAÇ

Bu prosedürün amacı, Bursa Uludağ Üniversitesi bünyesindeki Bilgi İşlem Daire Başkanlığı kapsamındaki güvenliğin bilgi sistemlerinin dâhili bir parçası olmasını sağlamak için güvenlik gereksinimleri ve güvenlik açıklarının takibi ile ilgili bir yöntem oluşturmaktır.

2. KAPSAM

Bu prosedür, Bursa Uludağ Üniversitesi bünyesindeki Bilgi İşlem Daire Başkanlığı için sistem temini, mevcut sistemlerin geliştirilmesi ve bakımı ile ilgili uygulama adımlarını kapsar.

3. TANIMLAR VE KISALTMALAR

Özel bir tanım bulunmamaktadır.

4. SORUMLULUK

Bu prosedürün işletilmesinden üniversitedeki tüm personel, BGYS Temsilcisi sorumludur.

5. UYGULAMA

5.1 Bilgi Sistemlerinin Güvenlik Gereksinimleri

5.1.1 Bilgi Güvenliği Gereksinimleri Analizi ve Belirtimi

Bilgi güvenliği ile ilgili gereksinimleri politikalar, yasal şartlar, BGYS olaylarının gözden geçirilmesi ve açıklıkların kontrolü ile belirlenir.
Yeni bilgi sistemlerine ihtiyaç oluşması durumunda bilgi sistemi için şartname oluşturularak kabul şartları belirlenir.
Bilgi sistemlerinin kabulü sırasında sözleşme ve teknik şartname olarak kontrol edildikten sonra işletmeye alınır.

5.1.2 Ağlara ve Ağ Hizmetlerine Erişim

Ağ ve ağ hizmetlerinin kullanımı ile ilgili aşağıdaki ilkeler benimsenmiştir.

- Ağ hizmetlerine erişim güvenlik duvarı üzerinden kontrol edilmektedir.
- Misafirler internet erişimleri misafir kullanıcı yönetimi ekranı uygulaması üzerinden yapılır.
- Kablosuz internet erişiminde sadece WPA2 şifre algoritması kullanılır.

5.1.3 Halka Açık Ağlardaki Uygulama Hizmetlerinin Güvenliğinin Sağlanması

Bilgi İşlem Daire Başkanlığında halka açık ağ üzerinde güvenlik sağlanmamaktadır.

5.1.4 Uygulama Hizmet İşlemlerinin Korunması

Uygulama hizmet işlemleri eksik bilgi iletimi, yanlış yönlendirme, yetkisiz mesaj değiştirme, yetkisiz ifşa, yetkisiz mesaj çoğaltma ve mesaj yeniden oluşturmayı engelleyecek şekilde yapılmıştır.

5.2 Geliştirme ve Destek Süreçlerinde Güvenlik

5.2.1 Sistem Değişiklik Kontrolü Prosedürleri

Geliştirme sistemleri üzerinde yapılacak değişiklikler yalnızca sanal bir işletim sistemi üzerinde test edildikten sonra yapılmaktadır.

5.2.2. İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirmesi

İşletim sistemi güncellemeleri geliştirme ortamlarına zarar vermemesi için BGYS temsilcisi tarafından sanal ortamda test edildikten sonra yapılmaktadır.

5.2.3. Yazılım paketlerindeki değişikliklerdeki kısıtlamalar

Yazılım paketlerinde yapılabilecek değişiklikler yalnızca BGYS Temsilcisi' nin onayı ile yapılmaktadır.

5.2.4. Güvenli Sistem Mühendisliği Prensipleri

Bilinen güvenlik açıkları tüm iş, veri, uygulama ve teknolojik sistemlerimiz üzerinde zarara yol açmaması için sürekli gözden geçirilir. Gerekli görülmesi durumunda yeni sistemlerin kullanımı için kaynaklar sağlanır.

5.2.5. Güvenli Geliştirme Ortamı

Kurumumuzda kullanılmakta olan geliştirme ortamları güvenli bir şekilde sağlanmaktadır.

5.2.6. Dışarıdan Sağlanan Geliştirme

Dışarıdan sağlanan sistem geliştirme faaliyeti bulunmamaktadır.

5.2.7. Sistem Güvenlik Testi

Sistem güvenlik testleri geliştirme süresince kontrol edilir. Sistem güvenlik testleri Bilgi ve İletişim Güvenliği Ekibi tarafından yapılır. Güvenlik işlevselliğini etkileyebilecek açıklıklar YGG toplantılarında görüşülür.

5.2.8. Sistem Kabul Testi

Sistem kabul testi yeni bir sistem yükseltmesi ihtiyacı olduğunda ya da yeni sürüm kabulünde yapılmaktadır. Sistem kabul testleri ilgili birim sorunluları tarafından yapılmaktadır.

5.3. Test Verisi

5.3.1. Test Verisinin Korunması

Test verisi yerel sunucular üzerinde saklanmakta ve korunmaktadır.

6. İLGİLİ DOKÜMANLAR

TS ISO / IEC 27001 Bilgi Güvenliği Yönetim Sistemi
TS ISO / IEC 27002 Bilgi Teknolojisi-Güvenlik Teknikleri Bilgi Güvenliği Yönetimi için Uygulama Kuralları