KONAK BELEDİYESİ BİLGİ İŞLEM MÜDÜRLÜĞÜ
VERİ GİRİŞİ GÜVENLİĞİ POLİTİKASI

AMAÇ

Madde 1 - Bu doküman, Konak Belediyesi'nde kullanılmak üzere geliştirilen tüm yönetim bilgi sistemi programlarına girilen her türlü verinin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması ve korunması amacıyla tüm kullanıcılar, yazılım sağlayıcılar, veritabanı ve sistem yöneticileri tarafından uyulması gereken kuralları ve kontrolleri tanımlamak üzere hazırlanmıştır.

KAPSAM

Madde 2 - Bu politika, Konak Belediyesinde bulunan bütün birimlerdeki personelin, bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

Veritabanı Güvenlik Politikası

Madde 3- Veritabanı güvenlik kuralları aşağıda belirtilmiştir.

3.1 Veritabanı sistemleri envanteri dokümante edilmeli ve bu envanterden sorumlu personel tanımlanmalıdır.

3.2 Veritabanı sistem kayıtları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.

3.3 Veritabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir.

3.4 Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı, yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.

3.5 Mevcut kullanılan Oracle program veritabanı yedekleri her gün sonunda, her ay sonunda ve her yılın son günü yedek olarak disk ve kasetlere alınmalı, yanmaz kasada saklanmalıdır.

3.6 Manyetik kartuş, DVD veya CD ortamlarında tutulan log kayıtları en az 2 (iki) yıl süre ile güvenli ortamlarda saklanmalıdır.

3.7 Veritabanı erişim politikaları "Kimlik Doğrulama ve Yetkilendirme" politikaları çerçevesinde oluşturulmalıdır.

3.8 Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.

3.9 Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.

3.10 Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.

3.11 Bilgi saklama medyaları kurum dışına çıkartılmamalıdır.

3.12 Sistem dokümantasyonu güvenli şekilde saklanmalıdır.

3.13 İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.

3.14 Sunucular direkt root kullanıcı erişimine kapatılmıştır. Sunuculara sadece SSH protokolü üzerinden yapılmalıdır.

3.15 Veritabanı sunucusuna ancak zorunlu hallerde “root” veya “admin” olarak bağlanılmalıdır. Root veya admin şifresi tanımlı kişi/kişilerde olmalıdır.

3.16 Bağlanacak kişilerin kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.

3.17 Bütün kullanıcıların yaptıkları işlemler kaydedilmelidir.

3.18 Sunucu ve veritabanı Admin şifreleri her ay değiştirilmeli ve şifreler yanmaz kasada saklanmalıdır.

3.19 Veritabanı sunucularına erişim belirli port, IP bilgileri ve yetkili kişiler üzerinden yapılmalıdır.

Yazılım Geliştirme Politikası

Madde 4- Yazılım Geliştirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

4.1 Sistem yazılımında mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.

4.2 Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.

4.3 İhtiyaçlar, uygun bir şekilde tanımlanmalıdır.

4.4 Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.

4.5 Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.

4.6 Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.

4.7 Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.

4.8 Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

Belgelendirme Politikası

Madde 5- Belgelendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

5.1 Bilişim sisteminin yapısı ile bütün iş ve işlemler açıkça belgelenmeli ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir durumda olmalıdır.

5.2 İş akışları uygun şekilde belgelenmelidir.

5.3 Belgeleme, tarih belirtilerek yapılmalı ve yedek kopyaları güvenli bir yerde muhafaza edilmelidir.

5.4 Bütün program değişikliklerinin detayları belgelenmelidir.

Kimlik doğrulama ve yetkilendirme politikası

Madde 6-Kimlik doğrulama ve yetkilendirme politikası ile ilgili kurallar aşağıda belirtilmiştir:

6.1 Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere erişeceği, resmi yazışmalar doğrultusunda belirlenerek yetkilendirme yapılır.

6.2 Kurum sistemlerine erişmesi gereken firma kullanıcılarına ait kimlikler ilgili profiller doğrultusunda yaratılır, işlem bitiminde kaldırılır.

6.3 Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veritabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenerek, denetim altında tutulur.

6.4 Tüm kurumsal sistemler üzerindeki kullanım hakları düzenli olarak gözden geçirilir ve bu gereksinimler gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilir.

6.5 Erişim ve yetki seviyelerinin sürekli olarak güncelliği sağlanır.

6.6 Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulur, tekrarlanan başarısız erişim istekleri/girişimleri incelenir.

Hilal Damla AYANLAR

Bilgi İşlem Müdürü