1. AMAÇ

T.C. Sağlık Bakanlığı Bingöl İl Sağlık Müdürlüğü ve bağlı tüm sağlık tesisleri bünyesindeki Web Uygulamaları geliştirme çalışmalarında uyulacak bilgi güvenliği politikasını tanımlamaktadır.

2. KAPSAM VE SORUMLULAR

T.C. Sağlık Bakanlığı Bingöl İl Sağlık Müdürlüğü ve bağlı tüm sağlık tesisleri bünyesinde Web Uygulamaları geliştirme çalışmaları yer alan tüm personeli kapsamaktadır.

3. UYGULAMA

3.1. Web, uygulama ve veritabanı sunucularının sistem bileşenleri hakkındaki kritik bilgiler (sunucu adı ve sürümü, kullanılan program sürümü v.b.) geliştirilen uygulama üzerinde gizlenir ve uygulamaya kullanan kullanıcılara gösterilmez.

3.2. Uygulamada oluşan hatalar ve uygulama sunucusu ön tanımlı hata mesajları kullanıcıya detaylı olarak gösterilmez.

3.3. Uygulamaların üzerinde koştukları sunucularda servis verdikleri dizinlerin içeriklerinin kullanıcılar tarafından listelenmemesi amacıyla gerekli konfigürasyon uygulama sunucusu üzerinde yapılır.

3.4. Arama motorları tarafından görüntülenmemesi istenen dizinler varsa, bunlar için robots.txt ile önlem alınır. Web Uygulamasına ait sayfalar içerisinde köprülenmeyen bağlantıların/dizinlerin (örneğin yönetim paneli adresi) güvenlik sorunu oluşturmaması adına robots.txt dosyasına eklenmez.

3.5. Ana sistem için gereksiz olan dosyalara (örneğin yedekleme, arşiv, test, geliştirme için kullanılan dosyalar) erişim engellenir ve sistemdeki gereksiz uygulamalar (örneğin ön tanımlı sunucu sayfaları, demo uygulamalar) kaldırılır.

3.6. Hassas bilgiler içeren web sayfalarının tarayıcılarda belleğe alınmaması için autocomplete, cache-control, pragma gibi gerekli HTTP/HTML başlıkları kullanılmalıdır.

3.7. Zayıf parolaların kullanımına izin verilmez. Kullanılan parolalar ve parolamı unuttum kontrol soru ve cevapları gibi diğer hassas veriler açık metin olarak saklanmaz.

3.8. Umumi olmayan bütün kaynaklara ve sayfalara erişim için sunucu tarafında kimlik doğrulaması yapılır.

3.9. Kullanıcılara (zarf, sözlü, e-posta yoluyla) dağıtılan başlangıç parolalar, kullanıcılar uygulamaya ilk giriş yaptıklarında değiştirilmeye zorlanır.

3.10. Kullanıcı adı ve parola ile kimlik doğrulamasının yapıldığı kontroller tek tip hata mesajı vermek suretiyle kullanıcı adları listeleme saldırılarına engel olmalıdırlar. Örnek bir hata mesajı "Girdiğiniz kullanıcı adı ve/veya parola yanlıştır." şeklinde olabilir.

3.11. Bütün başarılı ve başarısız login işlemleri ve kaynaklara erişim denemeleri kayıt altına alınır.

3.12. Oturum bilgisi zaman aşımına uğrayacak şekilde yapılandırılır.

3.13. Uygulamalarda başarılı kimlik doğrulama ve tekrarlayan kimlik doğrulama (re-authentication) neticesinde her zaman yeni bir oturum bilgisi oluşturulur. Çıkış işleminden sonra da var olan oturum bilgisi geçersizleştirilir.

3.14. Başarılı kimlik doğrulaması sonucu erişilen uygulamalarda sistemden tekrar çıkmak (logout) için gerekli linkler sağlanır.

3.15. Veritabanı kullanıcısının sadece uygulamanın kullandığı veritabanı kaynaklarına erişim hakkı sağlanır.

3.16. Yetki hakkının artık gerekmediği durumlarda (örneğin görevden ayrılma, projede rol değiştirme gibi) en kısa sürede ilgili haklar iptal edilmelidir.

3.17. Parola güncelleme işlemleri için eski parola her zaman sorulur.

3.18. Parola unuttum formları, gizli soru ve benzeri ek argümanlarla desteklenir.

3.19. Parola unuttum işlemlerinden sonra kullanıcıya gönderilen eposta, kullanıcı adı ve parola bilgisi içermez. Bunun yerine sınırlı yaşam süresi bulunan bir link gönderilip, o link üzerinden açılan sayfadan parola değiştirme işlemi gerçekleştirilir.

3.20. Uygulamalar, geliştirme ortamından uygulama ortamına aktarılırken gereksiz olan dosyalar (örneğin test kodlar, demo programlar, yedek dosyalar) silinir, şayet gerek yoksa kaynak kod aktarılmaz ve de aktarılacak olan kaynak kodlardaki yorum satırları silinir.

3.21. SQL enjeksiyonuna karşı veri kontrolü yöntemleri gerçekleştirilir.

3.22. Karşıdan dosya yükleme işlemlerinde yüklenilen dosya üzerinde isim, boyut, tip ve içerik kontrolü yapılır.

3.23. Kullanıcı parametrelerini kullanarak farklı sitelere yönlendirme yapan uygulamalarda ilgili parametrelere pozitif girdi denetimi uygulanmalı ve bu sayede olta saldırılarına engel olunur.

4. YAPTIRIM

4.1. Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla **BGYS Disiplin Prosedürü** Dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

Hazırlayan	Kontrol Eden	Onaylayan
Sedat ADEMOĞLU Bilişim Uzmanı	Songül BOĞATEMÜR Personel Hizmetleri Başk.Yard.	Uzm.Dr.Mehmet Emin GÜNDOĞDU İl Sağlık Müdürü