1. Uygulamalar kullanıcı hesaplarının yönetimini sağlayan ara yüzlere sahip olmalı ve bu ara yüzlere yalnızca yetkili kullanıcıların erişebilmesi sağlanmalıdır. Kullanıcı hesapları geçici veya kalıcı olarak kilitlenebilmelidir. Kalıcı olarak kilitlenen hesap, üzerindeki geçici kilit kaldırılsa dahi kilitli kalmalıdır.

2. Tüm başarılı ve başarısız kimlik doğrulama girişimleri için özet veri içerecek şekilde iz kaydı oluşturulmalıdır.

3. Tüm parola alanlarında kullanıcı giriş yaparken kullanıcının parolası varsayılan olarak maskelenmeli ve açık olarak görünmemelidir.

4. Unutulan parola işlevi ve diğer kurtarma yolları geçerli parolayı açığa çıkarmamalı ve yeni parola kullanıcıya açık metin olarak gönderilmemelidir.

5. İlk parola belirleme işlemi kullanıcı tarafından yapılmayacak ise, güvenli bir parola belirleme mekanizması ve üretilmiş bu parolaların güvenli olarak taşınması için iletme mekanizması oluşturulmalıdır. Ayrıca, bu parolalar ilk kullanımda değiştirilmeye zorlanmalıdır.

6. Kaynak kodda veya kaynak kod depolarında gizli bilgiler, API anahtarları ve parolalar yer almamalıdır. Kullanılan tüm kimlik doğrulama bilgileri şifrelenmeli ve korunan bir yerde depolanmalıdır.

7. Parola giriş alanları uzun ve karmaşık bir parola girilmesini engellememeli, parola cümle (deyimsel parola) kullanımına izin vermeli ya da teşvik etmelidir. Ayrıca parolalar için bir en uzun geçerlilik süresi tanımlanmış olmalıdır. Değişen parola fonksiyonu eski parolayı, yeni parolayı ve bir parola onayını kapsamalıdır.

8. Unutulan parolanın sıfırlaması kullanıcı adının unutulması vb. durumlar için; kısa ileti, e-posta onayı, mobil onay, çevrimdışı onay vb. yöntemler kullanılmalıdır. İlgili yöntemler kullanılırken sahip olunan, bilinen ve biyometrik faktörlerin en az ikisinden yararlanılmalıdır.

9. Tüm kimlik doğrulama ve yeniden kimlik doğrulama işlemleri sonucunda yeni bir oturum ve yeni bir oturum kimliği üretilmelidir. Oturum kimlikleri yeterince uzun olmalı, rastgele olmalı ve etkin oturumlar içerisinde tekil olmalıdır. Oluşturulan oturum kimliği yalnızca bir kez kullanılmalıdır.

10. Kimlik doğrulamayla erişilen tüm sayfalardan oturum kapatma işlevine erişilebilmelidir. Buna ek olarak, oluşturulan oturum kimliğinin geçerlilik süresi belirlenmelidir.

11. Geliştirilen uygulama/sistem kapsamında sunulan arayüzün kullanıcılar tarafından açıkça anlaşılabilir olması adına Türkçe dil desteği sağlanmalı, tedarik edilen ürünlerde ise Türkçe dil desteği olmalıdır.

12. Uygulama, yönettiği veriye ve kaynaklara erişimleri kayıt altına alabilmek için denetim kayıtları üretebilmelidir.

13. Veri tabanı üzerinde yetkili kullanıcılar tarafından gerçekleştirilen işlemler için denetim kayıtları oluşturulmalıdır. Bu kapsamda ilgili denetim politikaları/prosedürleri kurum ihtiyaçları doğrultusunda belirlenerek veri tabanı üzerinde uygulanmalıdır.

14. Uygulamanın sahip olduğu sistem ve yapılandırma dosyaları ile denetim kayıtları ve iz kayıtları gibi bilgiler kullanıcı verisiyle aynı konumda (dizin, sistem bölümü vb.) depolanmamalıdır.

15. Tüm formlarda istemci tarafında yapılan ön bellekleme işlevselliği kritik veri için kapatılmalıdır.

16. Güvenilmeyen kaynaklardan alınan dosyaların öncelikle türü ve içeriği doğrulanmalı, güvenlik açığına sebep olabilecek bir içeriğe sahip olup olmadığı kontrol edilmelidir.

17. Uygulamalar üzerinde sızma testleri, uygulama güvenliği testleri ve kaynak kod analizi yapılmalı veya yaptırılmalıdır.

18. Uygulamalar, tüm oluşabilecek hataları yakalayabilecek ve hata durumlarında varsayılan olarak güvenli durumlara geçecek şekilde tasarlanmış olmalıdır.

19. Uygulama, özel nitelikli kişisel veri içeren hata mesajı veya iz kaydı üretmemelidir. Hata durumu ile ilgili detaylar kullanıcıya gösterilmemelidir.

20. Siteler arası istek sahteciliği (CSRF) zafiyetine karşı gerekli güvenlik önlemleri (CSRF token, SameSite bayrağı vb.) alınmalıdır.

21. Bütün veri tabanı sorguları, parametrik olarak yapılmalı ve veri tabanına erişimde kullanılan dile karşı (SQL, NoSQL vb.) enjeksiyon saldırılarını engelleyebilecek güvenlik önlemleri alınmalıdır.

22. İşletim sistemi komut enjeksiyonu açıklarına karşı güvenlik önlemleri alınmalıdır.

23. Uygulama ve uygulamanın çalışma ortamında bellek taşması saldırılarına karşı önlem alınmalıdır.

24. Uygulama sunucusuna gelen isteklerin öngörülmeyen bir sayıda ya da büyüklükte olup olmadığı kontrol edilebilmelidir.

25. Anlaşma sona erdiğinde; taraflar, dokümanlarını karşılıklı olarak geri vermelidir.

26. Yazılımı yapan yüklenici kişisel verilerin mahremiyetini korumakla yükümlüdür. Firmanın şartname kapsamındaki verileri izinsiz kullanması, değiştirmesi veya çoğaltması, üçüncü kişilerle paylaşması yasaktır.

27. Uzak çalışma kapsamında uzak masaüstü bağlantısı yapılacaksa, şahısların kendilerine ait kişisel cihazlar veya sahibi bilinmeyen/herkes tarafından erişilebilen terminaller kullanılmamalıdır. Kullanıcıların bu tip terminaller üzerinden uzak masaüstü bağlantısı yaptıklarının tespit edilmesi halinde gerekli yasal ve idari yaptırımlar uygulanacaktır.

28. Sunucuya internet üzerinden erişime ihtiyaç olduğu durumlarda VPN üzerinden erişim sağlanmalıdır. VPN erişimi kurum politikalarına uygun olarak yapılmalıdır.

29. Kişisel veri üzerinde işlem yapılması ana amaç olmayan durumlarda (Adres bilgileri güncellenirken T.C. kimlik numarasının maskelenmesi, hesap numarasına havale işleminde alıcının adının maskelenmesi vb.) uygulama kişisel veriyi maskeleyerek göstermelidir.

30. İlgili kişiden alınmış açık rızanın inkâr edilemezliğini sağlamak amacıyla alınan açık rıza kayıt zaman damgası ile kayıt altına alınmalıdır.

31. Özel nitelikli kişisel verinin işlenmesi ve kişisel verinin üçüncü kişilere aktarılması durumunda açık rıza uygulama üzerinden alınmalı ve açık rıza beyan durumu sorgulanabilmelidir.

32. Açık Rıza ve Aydınlatma Metinleri, ilgili kişi tarafından okunup anlaşılacak kadar bir süre ekranda açık şekilde kalmalıdır. Yazılım, İlgili kişinin metinleri okumadan onaylamasına imkan vermemelidir.

33. Yazılımı yapan yüklenici, imzalayacağı BGYS-SZ03 GİZLİLİK SÖZLEŞMESİ ile kendisine devredilen işlerle ilgili her türlü bilgiyi (yazılım kaynak kodları, iş süreçleri, veri tabanı ile ilişkisel modeli gibi teknik dokümanları) gizli bilgi olarak kabul eder ve idarenin yazılı izni olmadan üçüncü kişilere vermemeyi, açıklamamayı, kamuya duyurmamayı, değiştirmemeyi, birbirlerinin yetkilendirdiği kişilerin hizmetin ifası sırasında gerekli erişimlerini engellememeyi ve bu şekilde meydana gelecek sair davranışlardan kaçınmayı taahhüt eder.

34. Tedarik edilen veya hizmet alımı ile geliştirilen uygulamalar için yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) içermediğine/içermeyeceğine dair üretici ve/veya tedarikçilerden BGYS-THH04 ARKA KAPI TAAHHÜTNAMESİ alınır.

35. Yüklenici bünyesinde çalışan ve şartname kapsamındaki verilere erişim sağlayan tüm personel BGYS-FRM30 3. TARAF BİREYSEL KULLANICI TAAHHÜT FORMU imzalamalıdır.