GÜVENLİ SUNUCU SERTİFİKASI
UYGULAMA KATMANI
TEKNİK ŞARTNAMESİ

SSL Sertifikası (Secure Sockets Layer – Güvenli Sunucu Sertifikası), bağlanılan web sitesinin kimliğinin doğrulamasını ve sunucuya gönderilen/alınan bilgilerin şifrelenerek aktarılmasını sağlayan dijital belge tipinde sertifikadır. Müdürlüğümüz ve bağlı birimlerinin resmi internet sitelerinde kullanılmak üzere SSL Sertifikası alımı yapılacaktır.

1. SSL Güvenli Sunucu Sertifikası OV SSL (Organization Validated SSL) özelliğine sahip olmalı, kurumsal doğrulama sağlamalıdır.
2. Wildcard özelliğine sahip olmalı, aynı alan adına bağlı sınırsız sayıda subdomain ve sunucuda kullanılabilmelidir.
3. En az 256 bit şifreleme ile yüksek güvenlik sağlamalıdır.
4. Uluslararası sertifika standartlarına uygun olmalıdır.
5. SSL Kök sertifikası Internet Explorer, Mozilla Firefox, Yandex, Google Chrome, Safari web tarayıcıları ile uyumlu olmalıdır.
6. Mobil cihazlar ile uyumlu olmalı, kök sertifikası Android ve IOS işletim sistemleri güncel sürümlerinin güvenilir köklerine eklenmiş olmalıdır.
7. Süre bitimine en az 1 ay kala kurum yetkilisine SMS ve/veya elektronik posta ile bilgilendirme mesajı gönderilmelidir.
8. Sertifika geçerlilik süresi 07.12.2026 tarihinde başlamak üzere 1 yıl olmalıdır.
9. Yüklenici aşağıda belirtilen bilgi güvenliği gereksinimlerini sağlamalıdır.
   9.1 Yüklenici ihaleye konu iş kapsamında ve garanti süresi boyunca yükümlüklerini yerine getirirken, Sağlık Bakanlığı bilgi güvenliği politikalarına uymak zorundadır. Bakanlığın bilgi güvenliği politikaları, Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzunda açıklanmıştır. Bahse konu dokümanlara internet üzerinden erişim sağlanabilmektedir.
   9.2 Yüklenicinin herhangi bir iş ve işleminde Bakanlık bilgi güvenliği politikalarına aykırı hareket etmesi halinde, bu durum İdare tarafından yazılı olarak yükleniciye bildirilir ve gerekli düzenlemeleri yapması istenir. Yükleniciye bu tarzda bir bildirim yapılmamış olması halinde, yüklenicinin bilgi güvenliği politikalarına uyduğu kabul edilir.
   9.3 Bakanlık bilgi güvenliği politikaları uyarınca, idareye ait bilgilerin korunması maksadıyla, yükleniciler ile "Kurumsal Gizlilik Taahhütnamesi" ve söz konusu iş kapsamında çalışacak olan yüklenici personeli ile "Personel Gizlilik Sözleşmesi" imzalanır.
   9.4 Sözleşmeye konu iş kapsamında alt yüklenici kullanılacaksa, ana yüklenici tarafından tüm alt yüklenicilere "Kurumsal Gizlilik Taahhütnamesi" imzalatılır ve taahhütnamelerin bir sureti idareye teslim edilir. Aynı şekilde alt yüklenici çalışanları ile de "Personel Gizlilik Sözleşmesi" imzalanır. Alt yükleniciler ve çalışanlarına ait sözleşmeler İdareye teslim edilmeden, alt yükleniciler çalışmalara katılamaz. Alt yükleniciler ile "Kurumsal Gizlilik Taahhütnamesi" imzalanması, asıl yüklenicinin gizlilik ile ilgili sorumluluklarını ortadan kaldırmaz veya değiştirmez.

9.5 Kurumsal Gizlilik Taahhütnamesi ve ihaleye konu iş kapsamında çalıştırılacak anahtar personelin Kişisel Gizlilik Sözleşmelerinin imza işlemleri tamamlanmadan, yüklenici tarafından işe başlanamaz.

9.6 Yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, Kişisel Gizlilik Sözleşmeleri idareye teslim edildikten sonra tanımlanır.

9.7 Destek faaliyetleri kapsamında KURUM bilişim sistemlerine uzaktan erişim yapılması ihtiyacı söz konusu olması halinde, Yüklenici FİRMA söz konusu kaynaklara erişimi İdare tarafından sağlanan VPN hizmeti üzerinden yapılır. VPN erişimi yapılabilmesi için Kurumsal Gizlilik Taahhütnamesi ve Personel Gizlilik Sözleşmelerinin idareye teslim edilmiş olması gerekir.

9.8 Temin edilen donanımların üzerindeki kalıcı veri barındırma imkânı olan disk/flaş bellek vb. depolama ortamlarında oluşan hata ve arızalar idarenin tesislerinde (yerinde) düzeltilecektir. Yerinde düzeltmenin mümkün olmaması nedeniyle söz konusu ortamların yükleniciye iade edilmesi ihtiyacı ortaya çıkar ise ortam üzerinde saklanan verilerin usulüne uygun olarak silinmeyi veya yok edilmeyi müteakip yükleniciye teslim edilecektir. Teknik nedenlerle silme veya yok etme işlemi yapılamıyorsa, söz konusu ortamlar yükleniciye teslim edilmeyecek ve yenisi ile değiştirilecektir.

9.9 06.07.2019 tarih ve 30823 sayılı Resmî Gazete 'de yayımlanarak yürürlüğe giren 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi'nin 12. Maddesi uyarınca; Tedarik edilecek yazılım, donanım ve cihaz/sistemlerde mevcut güvenlik önlemlerini aşarak erişim sağlamak üzere özel olarak tasarlanan ve/veya kasıtlı olarak dâhil edilmiş boşluklar veya güvenlik açıkları bulunmadığı konusunda yükleniciden örneği ekte verilen "Arka Kapı Taahhütnamesi " alınacaktır.

9.10 Arka Kapı Taahhütnamesi öncelikle üretici, üreticiden alınamıyorsa dağıtıcı, her ikisinden de alınamıyorsa yüklenici tarafından imzalanacaktır.

9.11 Arka Kapı Taahhütnamesi, taahhütnameyi imzalayacak tedarik zinciri bileşeni dikkate alınarak (üretici, dağıtıcı, yüklenici) her bir ürün için ayrı ayrı, (ürünlerin tür, tip, kullanım amacı, marka, model vb. özelliklerine göre gruplandırılarak) her bir grup için ayrı ayrı veya tüm ürünler için tek bir taahhütname olacak şekilde verilebilecektir.

9.12 Bu bölümde belirtilen kurumsal gizlilik taahhütnamesi, personel gizlilik sözleşmeleri ve arka kapı taahhütnamesi ihaleye konu tedarik sözleşmenin imzalanması sonrasında ihale üzerinde kalan yüklenici tarafından imzalanacak veya yukarıda belirtilen esaslar doğrultusunda ilgili kişi ve kurumlara imzalatılarak idareye teslim edilecektir. Bu belgeler ihaleye katılım için bir ön yeterlilik belgesi olarak istenmemiştir.

M. Mustafa YAĞMUR
Bilgisayar Mühendisi

Canberk SÖYLEMERT
Bilgisayar Teknikeri