WEB GÜVENLİĞİ YAZILIM TEKNİK ŞARTNAMESİ

1. İşin Adı ve Tanımı

WEB güvenliğinin şirket içinde kontrollü olarak sağlanması.

2. Amaç

Şirket tarafından sözleşmeye bağlanan web güvenliği İşinin yürütülmesinde uygulanacak genel esasları tespit etmektir.

3. İşin Kapsamı

Bu Şartname WEB güvenliğini yazılımını kapsar.

4. Tanımlar

Teknik Şartname içerisinde bahsi geçen aşağıdaki kelime ve deyimler bu bölümde belirtilen anlamları taşıyacaktır.

ŞİRKET: SAKARYA ELEKTRİK DAĞITIM A.Ş. Orhangazi Caddesi Trafo Tesisleri PK:160 54100 / SAKARYA

YÜKLENİCİ: Şartname kapsamındaki işleri yürütmekle görevli firmadır.

HİZMET: Bu Teknik Şartname kapsamında Yüklenicinin gerçekleştireceği bütün faaliyetlerdir.

KURULUM: Bu teknik şartname kapsamında olan ürün ve yazılımların belirtilen şekilde, proje planında belirtilen sürelerde, belirlenen Veri Merkezinde çalışır duruma getirilmesi.

5. İş Yeri: Sakarya Elektrik Dağıtım A.Ş.

6. İşin süresi: İşin süresi sözleşme imzası ile başlayacak olup 3(üç) yıl olacaktır.

7. Bildirimler ve Kalite Parametreleri

YÜKLENİCİ, ŞİRKET tarafından iletilen tüm bildirimlerin çözümlenmesi, sınıflandırılması, çözümlenmek üzere yönlendirilmesi ve çözümün takip edilmesi için YÜKLENİCİ'NİN ya da ŞİRKET'İN yardım masası uygulamasını kullanır. Hangisinin kullanılacağı ŞİRKET tarafından belirlenir ve değiştirilebilir.

Söz konusu Yardım Masası Uygulaması sayesinde ŞİRKET sorunları kaydedilir, tekrarlayan hatalar belirlenerek bunlar için kalıcı çözümler geliştirilir veya daha önce çıkan sorunlar taranarak daha hızlı çözümlenir. Böylece sistemlerin ve sunulan hizmetlerin tarihçesi de kaydedilerek problem yönetimi ve değişiklik yönetimi süreci altyapısı oluşturulur.

Hizmet Detayları	Açıklama	Miktar
Yıllık Bildirim Sayısı	Talep ve arıza bildirimleri	Sınırsız
7x24 Uzaktan Destek	Telefon, E-Posta, Uzak Masaüstü Bağlantısı vb.	Sınırsız
7x24 Yerinde Destek	İhtiyaç halinde yerinde destek	Sınırsız

Bildirim Önceliği	Açıklama	Bildirimden itibaren Çözüm Süresi
Acil Seviye Arıza	Hizmetin bütünüyle hizmet dışı kalmasına sebep olan problem.	2 Saat
Yüksek Seviye Arıza	Hizmetin bir alt parçasının hizmet dışı kalması veya bütünün normal hizmetini vermesine engel olan problem (bütünün normal hizmet vermesine engel performans problemleri acil öncelikli olarak değerlendirilir).	4 Saat
Orta Seviye Arıza	Hizmetin bütününün normal işleyişini engellemeyen ancak gerek performans gerekse az önemli alt servislerin hizmet vermesini engelleyen problem.	1 Gün
Düşük Seviye Arıza	Sistemin bütününün veya alt hizmetlerin normal işleyişini engellemeyen ancak ileride olabilecek bir problemi işaret eden sistem hataları.	2 Gün
Acil Seviye Talep	Yasal ve regülasyon zorunluluktan dolayı oluşan ve yapılacak işe kritik düzeyde etkisi olan talepler.	1 Gün
Yüksek Seviye Talep	İleride problem oluşturabilecek riskler taşıyan ve yapılacak işe yüksek düzeyde etkisi olan talepler.	3 Gün
Orta Seviye Talep	Alternatif bir çözüm uygulanabilecek durumlar ve hizmetin ana özelliklerini etkilemeyen talepler.	5 Gün
Düşük Seviye Talep	Servis fonksiyonlarına herhangi bir etki olmadığı durum veya bilgilendirme soruları.	10 İş günü veya karşılıklı mutabakat

8. Teknik Özellikler

Teklif edilecek çözümlerin yerel kurulum yada güncel teknolojileri destekleyecek şekilde çalışabilecek özellikte olmalıdır.

8.1. WEB GÜVENLİĞİ ve URL FİLTRELEME SİSTEMİ

8.1.1. Yazılım 750 kullanıcı lisansına sahip olacak ve bu lisans sözleşme tarihinden itibaren 3 yıl süreyle kuruma teslim edilecektir.

8.1.2. ŞİRKET, yazılımın 3 yıl süresince tüm güncelleme ve yeni yayınlanacak versiyonlarını (minör ve majör versiyonlar) bedelsiz olarak kullanım hakkına sahip olacaktır.

8.1.3. Herhangi bir lisans gereksinimi olmadan sistem Vmware Sanal Sistemler üzerinde çalışabilmelidir. Bunun için herhangi bir lisans limitasyonu veya ekstra maliyet bulunmamalıdır.

8.1.4. Yerel kurulum olması durumunda yedekli yapıda çalıştırılmak üzere yük dengeleme (load balancing) cihazlarıyla, Layer 4- 7 anahtarlama cihazlarıyla, WCCP protokolüyle veya round robin dns ile çalıştırılabilir olmalıdır. Transparent Proxy olarak kurum ağına konumlandırılabilmelidir.

8.1.5. Web Güvenlik bileşeni proxy/cache özelliğine sahip olmalı ve üzerinden geçen web trafiğinin Anti virus/malware kontrolünü sağlamalıdır.

8.1.6. Yazılım, tüm web trafiği içerisindeki zararlı uygulamalar, script tabanlı kodlar ve sayfa içerisine gizlenmiş (obfuscated) kodlara karşı koruma sağlamalıdır. Web sayfaları içerisinde bulunan ve kötü amaçlı içerik bulunduran sitelere verilen linkleri tespit edebilmeli ve bloklayabilmelidir.

8.1.7. Hem Inbound hem de Outbound trafiklerin analizlerini yapabilmelidir. Bu sayede bilgisayarların dışarıya doğru oluşan bağlantılarını tespit edebilmeli, Malware, Botnet ve Komuta Kontrol Merkezlerine doğru oluşan trafikleri bloklamalıdır. Sistem bu aktivitelere ait detaylı kayıtlar tutmalı ve bu durumdan etkilenmiş bilgisayarlar dashboard ekranlarında ve loglar içerisinden kolayca görülebilmelidir.

8.1.8. Zararlı kodlar içeren (spyware, web_borne viruses, Trojan horses, worms, script attacks, rogue internet code, botnet) web sayfalarına; data ve bilgi toplama ve tranfer etme, elektronik posta adresleri ve şifrelere erişme hakkına sahip olma gibi özellikler içeren sitelere erişimi kategorize edebilme, bloklama, izin verme veya sınırlı süre bağlantı imkânı sağlama gibi özelikler bulunmalıdır.

8.1.9. Güvenlik ile ilgili en az aşağıdaki kategorilere sahip olacaktır.

- Advanced Malware Command and Control
- Advanced Malware Payloads
- Compromised Websites
- Custom-Encrypted Uploads
- Files Containing Passwords
- Bot Networks
- Keyloggers
- Malicious Embedded Link
- Malicious Embedded iFrame
- Malicious Web sites
- Mobile Malware

- Phishing and Other Frauds
- Potentially Unwanted Software
- Potentially Exploited Documents
- Spyware
- Suspicious Embedded Link

8.1.10. Web güvenlik bileşeni, web üzerinden download edilen dosyaların da anti-virüs kontrolünü yapabilmelidir. Anti-virus kontrolünde devre dışı bırakılacak web siteleri tanımlanabilmelidir.

8.1.11. Yazılım, tehdit içerdiği önceden bilinen URL'ler için geniş bir veri tabanına sahip olmalıdır. Sistemi güvenlik tehditlerine karşı sürekli güncel olmalıdır, üretici internet üzerinde yeni keşfedilen güvenlik tehditleri için müşterilerindeki sistemleri sürekli güncel tutacak gelişmiş yeteneklere sahip olmalıdır.

8.1.12. En az 95 değişik kategori içerisinde güncel tehditleri barındırabilecek şekilde bloklama yapabilecek özellikte olmalıdır.

8.1.13. Yerel kurulum olması durumunda dinamik olarak gerçek zamanlı web sayfası taraması yapabilen ve kategorize edebilen motorlara sahip olmalı ve URL veri tabanında bulunmasa bile özellikle Web2.0 siteleri ve tehdit içeren siteler bloklanabilmeli, kurum URL filtreleme politikaları doğru bir şekilde uygulanabilmelidir. Dinamik kategorizasyon işlemi proxy bileşeni üzerinde gerçek zamanlı olarak yapılabilmeli, bu işlem sırasında herhangi bir dış (bulut sorgusu gibi) desteğe ihtiyaç duymamalıdır.

8.1.14. Politikalara uygun bir Web sayfası içerisinde, politikaları ihlal eden içerikler ayrıca bloklanabilmelidir.

8.1.15. SSL üzerinden gelebilecek zararlı kodların tespitinin yapılabilmesi için sistem SSL Decryption yapabilmelidir. Bu sayede SSL trafiği ile gidilen proxy siteleri tespit edilebilmelidir. Ayrıca belirli URL ve kategoriler SSL decryption işleminden hariç tutulabilmelidir. Bu iş için ayrı bir donanım ve/veya lisans gereksinimi olmamalıdır.

8.1.16. GhostSurf, BitTorrent, BoxCloud, JAP, Toonel, Tor, TeamViewer, VNC, LogMeIn gibi uygulamalar versiyon bilgilerinden bağımsız olarak tespit edilebilmeli ve bloklanabilmelidir.

8.1.17. Web hosting yapan sitelerde tüm siteyi değil, sadece istenmeyen sayfaları bloklamak için gerekli ayrımı yapabilmelidir.

8.1.18. İzin verilen anında mesajlaşma yazılımlarının içerisindeki dosya transferlerini algılayıp bloklayabilmelidir. (örn: MSN, Yahoo!, AOL, ICQ, NateOn Messenger Attachments)

8.1.19. Aynı site hem URL adresi hem de IP adresi bazında tanınabilmelidir. Kullanıcılar web sitesinin URL'i yerine IP adresini yazarak URL filtrelemeden kaçamamalıdır.

8.1.20. Politika tanımları için hazır gelen politikalar olmalı ayrıca sistem yöneticileri kendi politikalarını oluşturabilmelidir. Politika tanımları karışıklığa sebep olmayacak şekilde sade olmalı, açıklamalar içermelidir. Politikalar, haftanın belirli günlerinde belirlenecek zaman dilimlerinde farklı erişim politikaları atanabilmesine izin vermelidir. Zaman tanımlaması gün ve saat olarak tanımlanabilmelidir.

8.1.21. Kullanıcı ve gruplara özel politika tanımlanabilmesi için kullanıcı bilgisayarlarına ek bir yazılım gerektirmeden Active Directory ve LDAP sunucuları ile entegre çalışabilmelidir.

8.1.22. Yazılım yerel kurulumda Kerberos, NTLMv2 ve LDAP authentication desteklemelidir. AD entegrasyonu ile kişi grup bazlı kural yazılabilmelidir.

8.1.23. Mobil cihazlar için sertifika bazlı authentication desteklemelidir.

8.1.24. Kategorize edilmemiş, az hit alan siteleri, kullanıcı kategorize edebilmelidir. Mevcut database içerisinde kategorize edilmiş bir site, başka bir kategori altına kolaylıkla taşınabilmelidir.

8.1.25. Kullanıcıların gün içerisinde belirlenen kategoriler için kota (sınırlı süre) kullanmasına imkan verecektir.

8.1.26. Search Filtering özelliği sayesinde Google, Yandex, Yahoo, Bing gibi güçlü arama motorları içerisinde filtreleme yapabilmelidir. Bu arama motorları içerisinde aranan sözcükler için kullanıcıya filtrelenmiş sonuçlar getirmeli, istenmeyen içeriklere ait sonuçlar hiç sunulmamalıdır.

8.1.27. Yazılım, web filtreleme, güvenlik ve sistem yöneticisi kayıtlarını loglamaladır. Blokladığı/izin verdiği sitelere erişim isteklerinin detaylı logunu tutmalı ve istediğinde bu loglardan istatistiksel raporlar üretebilmelidir.

8.1.28. Log kayıtları, kullanıcı aktiviteleri, kullanıcı bilgileri ve hedef URL detaylarını içerecek şekilde gerçek zamanlı görüntülenebilir olmalıdır.

8.1.29. Yerel kurulumda yazılım, etkin raporlama için tüm bileşenlerinin desteklediği ortak bir veri tabanı kullanmalıdır. Raporlama veri tabanı için satır limitasyonu bulunmamalıdır. Veri tabanı olarak MS SQL 2008/2012/2014/2016 veri tabanlarını kullanabilmelidir.

8.1.30. Yerel kurulumda raporlamalar hem erişim sayısı (hit) hem de bant genişliği (bandwidth) kullanımı cinsinden olabilecektir.

8.1.31. Yazılım üzerinde kullanıcıların, grupların ve lokasyonların aktivitelerini, eğilimlerini gösterebilecek hazır raporlar bulundurmalıdır. Günlük, haftalık aylık otomatik rapor üretilebilmeli ve belirli kriterlere göre oluşturulan bu raporlar, otomatik olarak istenilen e-posta adreslerine gönderilebilmelidir. Sistem yöneticileri, tüm loglar üzerinden esnek bir şekilde gereksinimlerine uygun raporlar üretebilmelidir. Raporlar html, pdf veya xls formatında yada api entegrasyonu ile hazırlanabilmelidir.

8.1.32. Sistem yönetimi üzerinde kullanıcılara ait browser ve işletim sistemi versiyonları izlenebilmeli ayrıca user agent bilgileri görülebilmelidir.

8.1.33. Çözüm, kullanıcıların bulut uygulamaları kullanımlarını gösterebilen raporlara sahip olacaktır. Web erişim politikaları gibi, bulut uygulamalarına özel politikalar tanımlayarak kullanıcıların bulut uygulamalarına erişimlerini kontrol altına alabilecek yeteneklere sahip olacaktır.

8.1.34. Sistemin yönetimi ve raporları görmek üzere farklı yönetici seviyeleri ve roller tanımlanabilmelidir. Sadece raporlar ve istatistikleri kontrol etmek amaçlı idari yöneticiler için farklı rollerde yönetici tanımları yapılabilmelidir. Farklı kullanıcı

gruplarının, lokasyonlarının politika ve rapor yönetimi ilgili yöneticilere delege edilebilmelidir.

9. İşin İfası ile İlgili Şartlar (YÜKLENİCİ Sorumlulukları)

Lisans tanımı, kurulumu YÜKLENİCİ tarafından sağlanacaktır. İşin ifası aşamalarında hiçbir işlem adedi sınırı bulunmadan hizmet sürdürülecektir. YÜKLENİCİ desteğiyle beraber ŞİRKET'İN talep etmesi durumunda hiçbir bedel talep edilmeden Üretici desteği sağlanacaktır.

Web güvenliği yazılımı lisans kapsamındaki tüm özellik ve entegrasyonların çalışır duruma getirilmesi ve sürekliliğinin sağlanmasından Yüklenici sorumludur. Yüklenici Web güvenliği yazılımı güncel tehditlere karşı alınması gereken konfigürasyon değişikliklerini Şirkete sunmak ve uygun görülmesi halinde gerekli çalışmaların yapılmasından sorumludur. Yüklenici Web güvenliği kapsamında Şirket'in talep edeceği kural değişikliklerini ve/veya yeni kural çalışmalarını Şirket yapısını değerlendirerek yerine getirmekle yükümlüdür.

9.1. Arıza ve problemler ile ilgili bildirim, telefon veya elektronik posta ile ŞİRKET 'in talebi doğrultusunda, normal çalışma saatleri dışında da Yükleniciye iletilebilecektir. ŞİRKET, telefon ile destek hizmetlerini, YÜKLENİCİ 'nin bildireceği cep/çağrı merkezi telefonundan 7 gün 24 saat esasında sağlayacaktır.

9.2. YÜKLENİCİ sözleşmenin imzalanmasından itibaren 2-4 hafta içinde ürünlerin teslimatını gerçekleştirecektir.

9.3. YÜKLENİCİ, uygulaması tüm arayüzleri ile çalışır hale getirilerek ŞİRKET 'e teslim edilecektir.

9.4. YÜKLENİCİ kurulan yapıyı ve yapının çalışırlığını ayrıntılı bir şekilde anlatan dizayn dokümanını oluşturarak ŞİRKET 'e teslim edecektir.

9.5. YÜKLENİCİ, planlı bakım, yenileme, vb. gibi çalışmaların yapılması durumunda ŞİRKET'E en az 3 gün önceden haber verecektir. Acil bakım ve yenileme durumlarında ise süre kısıtı olmamakla birlikte ŞİRKET'E mutlaka önceden haber verilecektir.

10. Eğitim

Şartname kapsamındaki ürünler ile ilgili katılımcı sınırı olmadan yönetici eğitimi YÜKLENİCİ tarafından ücretsiz sağlanmalıdır. ŞİRKET'İN tekrar talep ettiği zamanlarda katılımcı sınırı olmadan YÜKLENİCİ tarafından sağlanacaktır. Yüklenici şartname özelindeki ürünler kapsamında en fazla 2 adet ile sınırlı olmak şartı ile üretici sertifikalı eğitimi sağlayacaktır.

11. Lisanslar

750 lisans YÜKLENİCİ tarafından sağlanacaktır.

12. Raporlama

12.1. Yüklenici 6 aylık periyotlar halinde ürünlerin olgunluk seviyesi ölçümü yapmalı ve ŞİRKET ile rapor paylaşılmalıdır.

12.2. Yüklenici 3 aylık periyotlar ile ürünlerin sağlık kontrollerini yaparak sistemlerin tüm yetenekleri ile çalışır durumda olduğu hakkında rapor hazırlayacak ve ŞİRKET ' e sunacaktır.

12.3. Ürün özelinde takip edilmesi gereken raporlar Yüklenici tarafından hazırlanarak ürün tarafından belirtilen e-posta gruplarına periyodik olarak gönderimi sağlanacaktır.

13. Garanti, Bakım ve Kabul

Garanti süresince YÜKLENİCİ ŞİRKET'ten hiçbir ücret talep edemez. Garanti kapsamında bakım, onarım, parça değişimi ve nakliye de dahil olmak üzere tüm masraflar YÜKLENİCİ tarafından karşılanır.

Garanti süresince ürüne müdahale yapılması gerektiğinde, mümkün ise ürünün kullanım yerinde gerekli müdahale yapılır.

13.1. Garanti Şartları ve Süresi

Ürün sözleşme süresi boyunca YÜKLENİCİ garantisi altında olup tüm talepler herhangi bir ek maliyet talep edilmeden YÜKLENİCİ tarafından karşılanacaktır.

13.2. Bakım

Ürünün güncellenmesi, yama geçilmesi vb. işlemler ŞİRKET talepleri doğrultusunda YÜKLENİCİ tarafından sözleşme kapsamında yapılacaktır.

13.3. Kesin kabul

Ürünün tüm entegrasyonları birlikte kurulması ve aktif olarak çalışır hale getirilmesi sonrasında ŞİRKET'in yazılı onayıyla kesin kabul yapılacaktır. Yaygınlaştırma işlemleri kesin kabul sonrasında devam edecektir.

14. Birim Fiyatlar ve Birim Fiyat Tarifeleri

15. İşin Yürütülmesi için Gerekli Personel ve Araç, Gereç ve Malzemeler

16. Teklif Fiyatına Dahil Olan/Olmayan Hususlar

17. Teslimat

18. Fiyat Farkları ile İlgili Hususlar

19. Yüklenicinin Çalıştırdığı Personel

19.1. Çevre sağlığı

Yüklenici ŞİRKET lokasyonlarda gerçekleştireceği işler esnasında tüm çevre kanun ve yönetmeliklerine uyarak, çevreyi koruyacak şekilde işlerini yürütmekle yükümlüdür.

19.2. İş Sağlığı ve Güvenliği

YÜKLENİCİ,

- Kanun ve yönetmeliklerde öngörülen her türlü önlemin yanında, o işyerinde iş güvenliğini sağlamak için gerekli olan ve bilimin, tecrübenin, teknolojinin imkân verdiği her türlü önlemi mevzuatta hükme bağlanmamış olsa da almakla,
- İşyerinde iş sağlığı ve güvenliği organizasyonu kurmak iş kazası ve meslek hastalığı risklerini tespit etmek ve bunlara karşı tedbir alınmasını sağlamak,

- İşyerinde güvenli bir şekilde çalışılmasını sağlamak üzere gerekli kontrollerin yapılmasını koordine etmek,
- Hizmete konu olan işle ilgili çalışanlarına mevzuatın zorunlu kıldığı süre ve nitelikte İSG eğitimi ve mesleki eğitimleri vermek,
- İşin yürütülmesi esnasında gerekli her türlü sağlık ve güvenlik önlemlerini (ortam güvenliğini sağlamak, uygun kişisel koruyucu donanımları temin etmek vb.) almak,
- Periyodik kontrol ve muayene gerekliliği olan malzeme, ekipman, KKD bulunması durumunda, gerekli kontrollerin periyodik olarak yapılmasını sağlamak ve kayıt altına almak,
- Çalışanların sahada tanımlanmış İSG kurallarını uygulamalarını güvence altına almak için gözetim ve denetimler yapmak ve istendiğinde gösterilmek üzere bu gözetim ve denetimleri kayıt altına almış olmak,
- ŞİRKET taşınmazları içerisinde görev yapan çalışanlarının ŞİRKET Ziyaretçi Aydınlatma Metnini imzalamasını sağlamak,
- İSG mevzuatı gereği tüm kayıtları muhafaza etmek,
- Sözleşmeye uygunluğu takip etmek ile yükümlüdür.

19.3. Ayrım

YÜKLENİCİ, elemanları kişilik özelikleri veya inançları temelinde değil, işi yapabilme becerilerini esas alarak; din, dil, ırk, renk, cinsiyet, uyruk, yaş, hamilelik veya medeni durum ayırımı yapmaksızın istihdam edecektir.

Aynı zamanda tüm çalışanlarına ücret ve sosyal haklar sağlarken; din, dil, ırk, renk, cinsiyet, uyruk, yaş, hamilelik veya medeni durum ayırımı yapmayacaktır.

19.4. Zorla Çalıştırma

YÜKLENİCİ, herhangi bir şekilde insan ticaretine iştirak edemez, zorla, gönülsüz ve köle işçi çalıştıramaz ve bu tür eleman çalıştıran şirketlerden malzeme veya hizmet satın alamaz.

19.5. Çocukların Çalıştırılması

YÜKLENİCİ, 18 yaşını doldurmamış çalışanı kesinlikle istihdam etmeyecektir.

19.6. Birlik Kurma Özgürlüğü

YÜKLENİCİ çalışanları; yasalara uygun şekilde birlik kurma veya kurulmuş olanlara katılma özgürlüğüne sahiptirler.

20. Yönetim Sistemi

YÜKLENİCİ, yürürlükte bulunan yasalara, düzenlemelere ve ŞİRKET'İN ilkelerine uygun bir yönetim sistemine sahip olmalı, bu sistemin sürekli bir şekilde geliştirilmesi ve değişen yasalara ve düzenlemelere uyacak şekilde uyumluluğu sağlamaları gerekmektedir.

ŞİRKET hizmet sağlayan Yüklenicilerine, Kalite (ISO9001), Çevre (ISO14001), İş Sağlığı ve Güvenliği (ISO 45001) vb. sistemleri sağlamalarını tavsiye etmektedir.