SUNUCU UÇ NOKTA GÜVENLİĞİ YAZILIMI

1. İşin Adı ve Tanımı

Sunucu sistemleri işletim sistemi güvenlik yazılımı alımı.

2. Amaç

ŞİRKET'in tüm sunucu sistemlerinde kullanılma üzere işletim sistemi güvenlik yazılımı temin edilecektir.

3. İşin Kapsamı

ŞİRKET' in mevcut windows ve linux işletim sistemine sahip sunucularında kullanılmak üzere işletim sistemi güvenliğinin sağlanması için gerekli güvenlik yazılımı ve desteğinin satın alınmasıdır.

4. Tanımlar

5. İş Yeri:

6. İşin süresi: 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'nin ya da ŞİRKET'in 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 Müdahale Süresi
Acil Seviye Arıza	Hizmetin bütünüyle hizmet dışı kalmasına sebep olan problem.	4 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).	8 Saat

Orta Seviye Arıza	Hizmetin bütününün normal işleyişini engellemeyen ancak gerek performans gerekse az önemli alt servislerin hizmet vermesini engelleyen problem.	2 Gün
Düşük Seviye Arıza	Sistemin bütününün veya alt hizmetlerin normal işleyişini engellemeyen ancak ileride olabilecek bir problemi işaret eden sistem hataları.	5 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

8.1. Sunucu Güvenliği

8.1.1. Teklif edilecek Sunucu Güvenlik Yazılımını oluşturan tüm bileşenler aynı üreticiye ait tek bir ürün olacaktır. Aynı üreticiye dahi ait olsa farklı ürünlerin bir araya getirilmesinden oluşturulan bir çözüm olmayacaktır.

8.1.2. Teklif edilecek Sunucu Güvenlik Yazılımı fiziksel, sanal ve bulut ortamdaki sunucu sistemlerin güvenlik politikalarını tek bir noktadan yönetebilecek özellikte olacaktır.

8.1.3. Teklif edilecek Sunucu Güvenlik Yazılımı Merkezi Yönetim Sistemi ve İşletim sistemi ajan uygulamalarından oluşacaktır.

8.1.4. Teklif edilecek Sunucu Güvenlik Yazılımı aşağıdaki işletim sistemi platformlarında çalışabilecektir:

- Microsoft Windows
- Red Hat Enterprise Linux
- CentOS Linux
- Rocky Linux
- Oracle Linux
- SUSE Linux
- Ubuntu Linux
- Debian Linux
- AlmaLinux
- Solaris
- AIX

8.1.5. Teklif edilecek Sunucu Güvenlik Yazılımı yüksek erişilebilir mimaride çalışmayı desteklemelidir.

8.1.6. Teklif edilecek Sunucu Güvenlik Yazılımı Merkezi Yönetim Sistemi Linux ve Windows işletim sistemleri üzerinde çalışmayı destekleyecektir.

8.1.7. Teklif edilecek Sunucu Güvenlik Yazılımı Merkezi Yönetim Sistemi veritabanı olarak Oracle ve Microsoft SQL Server ile çalışmayı destekleyecektir.

8.1.8. Teklif edilecek Sunucu Güvenlik Yazılımı üzerinde saldırı tespit ve önleme, güvenlik duvarı, zararlı yazılım önleme, web sitesi güvenilirliği, bütünlük gözleme, kütük inceleme ve uygulama kontrolü bileşenleri bulunacak, bu işlevlerle ilgili tüm bileşenler teklif edilecektir.

8.1.9. Teklif edilecek Sunucu Güvenlik Yazılımı üzerinde bulunacak saldırı tespit ve önleme bileşeni gelen ve giden trafiği tarayabilecek ve derin paket inceleme (DPI) çalışabilecek mimaride olacaktır.

8.1.10. Teklif edilecek Sunucu Güvenlik Yazılımı, sanal yama (host based IPS) özelliğini barındıracaktır. Sanal yama özelliği ile sunucular üzerinde bulunan ağ zafiyetleri tespit edilebilecek, isteğe bağlı olarak manuel ve otomatik olarak kapatılabilecektir.

8.1.11. Teklif edilecek Sunucu Güvenlik Yazılımı üzerinde bulunacak olan güvenlik duvarı, keşif taramalarını engelleme yeteneğine sahip olmalıdır. Bu güvenlik duvarı ile MAC, IP, Protokol, Port bazlı erişim kuralları uygulanabilecektir.

8.1.12. Teklif edilecek Sunucu Güvenlik Yazılımı üzerinde bulunacak bütünlük gözleme bileşeni kritik işletim sistemi dosyaları, dizinleri, kayıt defteri (registry) anahtar ve değerlerindeki değişiklikleri gerçek zamanlı izleyerek rapor edebilecek, alarm üretebilecektir.

8.1.13. Teklif edilecek Sunucu Güvenlik Yazılımı üzerinde bulunacak zararlı yazılım önleme bileşeni aynı üreticiye ait davranış tabanlı analiz motorunu kullanacaktır. Üçüncü taraf bir üreticiye ait motor kullanmayacaktır.

8.1.14. Teklif edilecek Sunucu Güvenlik Yazılımı üzerinde bulunacak kütük inceleme bileşeni çalıştığı işletim sistemi üzerindeki işletim sistemi ve uygulamalara ait günlük kayıtları ve kütükleri izleyerek şüpheli durumları rapor edebilecek, alarm üretebilecektir.

8.1.15. Teklif edilecek Sunucu Güvenlik Yazılımı uygulama kontrolü özelliği ile işletim sistemi üzerinde çalışan uygulamalarda beyaz liste ve kara liste oluşturabilecektir. Bu modül mevcut envanteri çıkarıp ona izin verecek ve sonrasındaki yeni gelen veya değişen uygulamaları bloklayabilecektir.

8.1.16. Teklif edilecek Sunucu Güvenlik Yazılımı sanal yama, kütük inceleme ve bütünlük gözleme bileşeni için sunucuda bir keşif taraması yaparak çalışan uygulama ve rollere göre otomatik olarak kurallar önerebilecektir. Böylece her sunucu için o sunucuya özgü bir kural setini otomatik olarak uygulayabilecektir.

8.1.17. Teklif edilecek Sunucu Güvenlik Yazılımı VMware NSX ile entergre çalışabilecektir ve sunucularda ajansız koruma sağlayabilecektir.

8.1.18. Teklif edilecek Sunucu Güvenlik Yazılımı üreticinin Global Tehdit İstihbarat hizmetine erişebilecek, bu hizmet sayesinde web sayfaları, elektronik posta kaynakları ve dosyalar için saygınlık sorguları yapabilecektir.

8.1.19. Teklif edilecek Sunucu Güvenlik Yazılımı, aynı üreticinin Gelişmiş Saldırılar İçin Detaylı Analiz Sistemi ile entegrasyonu destekleyecektir. Bu entegrasyon ile şüpheli gördüğü dosyaları analize gönderebilecektir. Ayrıca analiz sonucu bulunan dosya ve URL leri bloklayabilecektir.

8.1.20. Teklif edilecek Sunucu Güvenlik Yazılımı “docker” içeren bir işletim sistemi içinde çalışan konteynerlar için antivirüs, IPS ve firewall korumasını destekleyecektir. Aynı işletim sistemi içindeki iki konteyner arasındaki trafiği inceleyebilecek ve atakları bloklayabilecektir.

8.2. Uç Nokta Güvenliği

8.2.1. Teklif edilecek uç nokta güvenlik yazılımı davranış analizine ve makine öğrenmesine dayalı bir tehdit izleme, engelleme ve aksiyon alma aracı olmalıdır.

8.2.2. Teklif edilecek uç nokta güvenlik yazılımı alarm üretebildiği her tehdit için engelleme ve aksiyon alma özelliğini sunmalıdır.

8.2.3. Teklif edilecek uç nokta güvenlik yazılımı ile uç nokta cihazında yer alan dosya, IP adresi, hash, process, bilgisi vb gibi aramalar yapılabilmelidir. Arama yetenekleri manuel tehdit avcılığına imkan sağlamalıdır. Arama yetenekleri neticesinde tüm envanterde belirtilen arama kriterleri ile arama yapılabilmeli ve kısa sürede cevap alınabilmelidir.

8.2.4. Ajan dağıtımı SCCM, GPO gibi altyapılar ile dağıtılabilmeli ve raporlanabilmelidir.

8.2.5. Teklif edilecek uç nokta güvenlik yazılımı içerisindeki bilgisayarlar farklı özelliklerine göre mantıksal olarak gruplanabilmelidir; etiketleme, risk skorlama gibi yöntemler bulunmalıdır.

8.2.6. Teklif edilecek uç nokta güvenlik yazılımı yönetim paneli ile gerçekleştirilen veri trafiği güvenli bir standart protokol kullanarak gerçekleştirilmelidir.

8.2.7. Teklif edilecek uç nokta güvenlik yazılım mevcutta kullanılan SIEM çözümü ile entegrasyonunun olması gerekmektedir.

8.2.8. Teklif edilecek uç nokta güvenlik yazılımı zararlı aktivite girişimin öncesinde, esnasında ve sonrasında tespit ve engelleme yeteneklerine sahip olmalıdır.

8.2.9. Teklif edilecek uç nokta güvenlik yazılımı üzerine raporlanan davranışlardan yola çıkılarak hedefe yönelik siber saldırıların (APT) analizi yapılabilmeli, herhangi bir şekilde etkilenen uç nokta var ise burada gerçekleştirilmesi gereken müdahaleler ile ilgili yol gösterilmelidir. Elde edilen veriler farklı katmanlarda kullanılmak üzere dış dünyaya alınabilmelidir. Aynı yöntemle dış dünyadan IOC (indication of compromise), hash, IP, filename vb veriler tehdit verisi olarak işlenebilmelidir. Bu verilere yönelik alarmlar oluşturulabilmeli ve aksiyonlar alınabilmelidir.

8.2.10. Karşılaşılan saldırı vektörünün hedefli bir saldırı mı yoksa genel bir atak mı olduğu hususunda bilgi vermelidir.

8.2.11. Teklif edilecek uç nokta güvenlik yazılımı zararlı aktivitenin en başından sonuna kadar devam eden bir aktivite raporu sunabilmeli, haberleşilen C&C sunucuları, network aktiviteleri, yerel değişiklikleri raporlayabilmelidir.

8.2.12. Komut satırı, powershell, bash, pyhton, VMI, VBS vb her türlü script aktivitesi ve komutlar üzerinden gelen ataklara karşı aksiyon alabilmelidir.

8.2.13. Teklif edilecek uç nokta güvenlik yazılımı üzerinde isteğe bağlı tanımlamalar (whitelist / blacklist vb gibi) gerçekleştirilebilmelidir. Teklif edilecek Teklif edilecek uç nokta güvenlik yazılımı, özelleştirilmiş IOC tanımı ile sadece zararlı davranışlarda değil, güvenlik yöneticilerinin belirlediği durumlarda da alarm üretebilmeli ve aksiyon alabilmelidir. Varsayılan olarak gelen tespit ya da koruma kuralları düzenlenebilmelidir.

8.2.14. Teklif edilecek uç nokta güvenlik yazılımı üzerinde ortaya çıkan tehditler kolaylıkla incelenebilir, anlaşılabilir ve detaylı olmalıdır.

8.2.15. Teklif edilecek uç nokta güvenlik yazılımı üzerinde ortaya çıkan tehditlere karşı manuel müdahale imkânı bulunmalıdır. (network izolasyonu, AV tetiklenmesi vb gibi)

8.2.16. Teklif edilecek uç nokta güvenlik yazılımı hem yönetim ara yüzünden veya ajan üzerinden API desteği sunmalı, gerekli görüldüğü durumlarda çeşitli aksiyonları toplu olarak alabilmeli, toplu veri toplanmasına imkân vermelidir.

8.2.17. Teklif edilecek uç nokta güvenlik yazılımı, kuruluşun ağından çevrimdışı olan uç noktalar için tam koruma sağlamalıdır.

8.2.18. Teklif edilecek uç nokta güvenlik yazılımı, sunduğu arayüzde ortaya çıkan tehditleri kolaylıkla incelenebilir, anlaşılabilir ve detaylı olmalıdır. Bilgi vermenin yanında iyileştirme önerileri de sağlanmalıdır.

8.2.19. Teklif edilecek uç nokta güvenlik yazılımı, uyarılar durumunda güvenlik personelini bilgilendirme sağlamalıdır.

8.2.20. Teklif edilecek uç nokta güvenlik yazılımı, yetkisiz kullanıcıların erişimine ve manipülasyonuna karşı dahili bir koruma mekanizmasına sahip olmalıdır.

8.2.21. Teklif edilecek uç nokta güvenlik yazılımı, yaygın saldırı araçlarının (Metasploit, Empire, Cobalt vb.) Kullanımını tanımlamalı ve engellemelidir.

8.2.22. Teklif edilecek uç nokta güvenlik yazılımı, ayrıcalık yükseltme saldırılarını tanımlamalı ve engellemelidir.

8.2.23. Teklif edilecek uç nokta güvenlik yazılımı, komut satır sorgu içeriğini görebilmeli. (Cmd ve Powershell komut içeri tespiti)

8.2.24. Teklif edilecek uç nokta güvenlik yazılımı, uç noktalarda kötü niyetli varlık ve faaliyetlerin yalıtılmasını ve azaltılmasını desteklemelidir.

Koordine edilmiş bir komutu (CMD arayüzü gibi) çalıştırma özelliği.

Bir ağ konumundan komut dosyası veya dosya çalıştırmak veya bir ağ sürücüsü bağlamak.

Uç nokta / sunucu kapatma.

Uç noktanın / sunucunun ağdan izole edilmesi. (yönetim uygulamasının erişimi kesilmeden)

Dosya silme (etkin çalışma dosyaları dahil).

Dosya karantinaya alma (etkin çalışma dosyaları dahil).

İşlem durdurma

Bir hizmetin ve zamanlanmış görevin kaldırılması ve / veya silinmesi.

Yerel kullanıcı hesabını veya etki alanı kullanıcısını kilitleme.

Hedefe dayalı iletişimi engelleme (etki alanı adresi veya IP adresi).

8.2.25. Teklif edilecek uç nokta güvenlik yazılımı, ortamdaki tüm kuruluşlar ve faaliyetleri hakkında sürekli veri toplamalıdır.

(a) Dosya etkileşimi (oluşturma, açma, yeniden adlandırma, silme, yürütme)
(b) İşlem yürütme (işlem ağacı ekranı dahil).
(c) Kullanıcı Girişi.
(d) Ağ trafiği.
(e) Kayıt defteri değişiklikleri.
(f) Yüklü yazılım.

9. İşin İfası ile İlgili Şartlar (YÜKLENİCİ Sorumlulukları)

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.

9.1 Bakım ve destek anlaşması kapsamında, kurulmuş olan sistemin sorunsuz çalışması için gerekli olabilecek değişiklik, güncelleme vb. işlemleri ve yeni yazılım/bileşenlerin kurulumu ve devreye alımı ŞİRKET 'in yetkili personeli gözetiminde Firma tarafından gerçekleştirilecektir.

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

9.3 YÜKLENİCİ, tüm yazılım ürünlerinin, onarım, yama (patch) ve temel sürümleri dahil, güncelleştirilmiş veya değiştirilmiş bütün yeni versiyonlarını, ŞİRKET’e sunacaktır. Bu hizmete, yenilenmiş kullanım kılavuzları ve sürüm notlarının temini de dâhildir. YÜKLENİCİ‘nin çalışmakta olan sisteminde yazılım güncelleştirmesinin yapılıp yapılmayacağı kararı, ŞİRKET tarafından verilecektir.

9.4 YÜKLENİCİ, oluşturulacak yapıyla ilgili bilgilerin sağlanmasının yanı sıra, ŞİRKET‘in gelecekteki ihtiyaçları doğrultusunda konfigürasyon değişiklikleri, donanım/yazılım değişiklikleri/güncelleştirilmesi, var olan yapıya entegrasyonu konularında danışmanlık hizmetlerini verecektir.

9.5 ŞİRKET, destek ihtiyacının karşılanması için sınırsız çağrı açabilme hakkına sahip olacaktır.

9.6 YÜKLENİCİ, uygulamanın başarılı bir şekilde hizmete hazır ve çalışır hale getirilmesi için gerekli plan, kurma ve konfigürasyonu, sistem entegrasyonu, işletime alınması ve eğitimi ile ilgili tam bir uygulama planını ŞİRKET ‘e verecektir.

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

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

9.9 Donanımlar ve yazılımlara ilişkin CD’ler ve ilgili tüm dokümanlar ile lisans bilgileri ŞİRKET ‘e eksiksiz teslim edilecektir.

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

9.11 Tüm eğitimler, YÜKLENİCİ tarafından sağlanacak olup, eğitimler YÜKLENİCİ tarafından sertifikalandırılmış yetkin personel tarafından verilecektir.

9.12 YÜKLENİCİ tarafından verilen eğitimlerin yetersiz veya başarısız bulunması durumunda ŞİRKET 'in talebi üzere eğitimler ücretsiz olarak tekrarlanacaktır.

9.13 YÜKLENİCİ, ŞİRKET’E sağladığı hizmetler için 7 gün 24 saat hizmet veren müşteri hizmetleri servisi sunacaktır.

9.14 YÜKLENİCİ, hizmeti etkileyen bir arıza veya hata tespit ederse ŞİRKET’in ihbarına gerek duymaksızın, ŞİRKET’e bildirerek arızaya müdahale edebilecektir. YÜKLENİCİ, gerektiğinde ŞİRKET’le işbirliği içerisinde arızanın sebebini ve niteliğini belirlemek için testler yapacak, arızayı tespit etmek ve sorunu gidermek için yapılması gereken faaliyetler hakkında mutlaka ŞİRKET’İ bilgilendirecektir.

9.15 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.

Talep edilen hizmetler kapsamında YÜKLENİCİ tarafından ŞİRKET’E temin edilen tüm donanım, yazılım ve ekipmanlar sözleşme süresince YÜKLENİCİ’nin bakım ve destek garantisinde olacaktır.

10 Eğitim

Şartname kapsamında alınmış olan ürünlere yönelik yönetici eğitimleri ŞİRKET’İN talep ettiği zamanlarda katılımcı sınırı olmadan YÜKLENİCİ tarafından ŞİRKET faaliyet alanında bulunan lokasyonlarda veya ŞİRKET ‘in uygun bulması durumunda online olarak sağlanacaktır. Yüklenici şartname kapsamında alınacak ürünün üreticisinden en az 2 kişilik olacak şekilde üretici sertifikalı eğitim temin edecektir.

11 Lisanslar

Lisans bilgileri ŞİRKET'e eksiksiz teslim edilecektir.

12 Raporlama

YÜKLENİCİ tarafından sağlanacak hizmet kapsamında ele alınan alt hizmetler ve/veya birimler için kullanılabilirlik (erişim), ölçüm, raporlama, çağrı cevaplama, bakım ve istisnai durumlar için gerekli detaylar talep edilmesi durumunda sağlanabilir olacaktır. 6 ayda bir yapılan sistemlerin sağlık ve en iyi konfigürasyon kontrolleri sonucu ŞİRKET ' e raporlanacaktır.

13 Garanti, Bakım ve Kabul

Garanti süresince YÜKLENİCİ ŞİRKET' ten hiçbir ücret talep edemez. Garanti kapsamında bakım ve destek olmak üzere tüm masraflar YÜKLENİCİ tarafından karşılanır.

13.1.1 Garanti Şartları ve Süresi

İlgili yazlım garanti süresi 3 yıl olacaktır.

13.1.2 Bakım

İş kapsamında, periyodik olarak veya ŞİRKET'in talebi üzerine yazılımın kararlı sürümünün bir üst versiyona geçişi gibi gerekli güncelleme ve bakım desteği YÜKLENİCİ tarafından ücretsiz olarak sağlanacaktır. Tüm versiyon geçişleri ve güncelleme işlemleri, ŞİRKET tarafından belirlenen ve YÜKLENİCİ ile mutabık kalınan zamanda gerçekleştirilecektir.

13.1.3 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

Sözleşmenin amir hükümleri geçerlidir.

17 Teslimat

Sözleşmenin amir hükümleri geçerlidir.

18 Fiyat Farkları ile İlgili Hususlar

Sözleşmenin amir hükümleri geçerlidir.

19 Yüklenicinin Çalıştırdığı Personel

19.1 Çevre sağlığı

Yüklenici Şirket lokasyonlarda gerçekleştireceği işler esnasında tüm çevre kanun, tüzük 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,
- SEDAŞ taşınmazları içerisinde görev yapan çalışanlarının SEDAŞ 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 SEDAŞ'ın ilkelerine uygun bir yönetim sistemine sahip olmalı, bu sistemin sürekli bir şekilde geliştirilmesi ve değişen yasalara ve düzenlemelere uyacak şekilde uyumluluğu sağlamaları gerekmektedir.

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