



## Güvenlik Farkındalığı ve Olay Yönetimi Yazılım Alımı Teknik Şartnamesi

### 1. İşin Adı ve Tanımı

Güvenlik Farkındalığı ve Olay Yönetimi Yazılım Alımı.

### 2. Amaç

İnsan, süreç ve teknoloji odaklı bütünsel bir yaklaşım ile, internet üzerinden gelen tehditlere karşı siber güvenlik farkındalığı oluşturan sosyal mühendislik ve ortalama saldırılarına karşı, kullanıcıların dikkat ve farkındalık düzeyini artırmayı, teknolojik önlemlerin yeterliliğini test etmeyi, olay müdahale ortamı sunmayı amaçlamaktadır.

### 3. İşin Kapsamı

Şirket çalışanları tarafından bildirilen ortalama tehditlerini, postalarını işleme ve bu tehditlere müdahale işlemlerini hızlandırmak ve ihlal riskini azaltmak için ihtiyaç duyulan görünürlük ve analitik verilerini sağlanması. Şirket BT güvenlik operasyonları ekiplerinin ve/veya olay müdahale ekiplerinin, Şirketin halihazırda kullandığı e-posta güvenlik teknolojilerini / çözümlerini atlatan ortalama (phishing) tehditlerinin öncelik sırasına sokulmasını, analizini ve müdahalesini otomasyona bağlamalarına olanak sağlayan platformun edinilmesi.

### 4. Tanımlar

**ŞİRKET:** SAKARYA ELEKTRİK DAĞITIM A.Ş.

**YÜKLENİCİ:** Şartname kapsamındaki işleri yürütmekle görevli firmadır.

**HİZMET:** Bu Teknik Şartname kapsamında Yüklenicinin gerçekleştireceği bütün faaliyetlerdir.

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

### 5. İş Yeri:

-

**6. İşin süresi:** Sözleşme taslağında belirtildiği gibidir.

### 7. Bildirimler ve Kalite Parametreleri

YÜKLENİCİ, ŞİRKET tarafından iletilen tüm bildirimlerin çözülmesi, 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 Kalitesi beklentisi aşağıdaki tablolar ile özetlenmiştir.

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.	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 bütününe normal işleyişini engellemeyen ancak gerek performans gerekse az önemli alt servislerin hizmet vermesini engelleyen problem.	2 Gün
Düşük Seviye Arıza	Sistemin bütününe 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

8.1.1. Kurumun iç ağında çalışma özelliği (on-premise) olacak ve YÜKLENİCİ tarafından belirtilen ön gereksinimler sağlandığı takdirde fiziksel yada sanallaştırma platformlarında Linux temelli işletim sistemlerinde çalışmalıdır.

8.1.2. Hybrit (on-premise ve cloud) çalışma özelliği olmalıdır.

8.1.3. Platformun ürettiği tüm olay kayıtları merkezi log sunucusuna iletilebilmelidir.

8.1.4. Platformun yönetimi için minimum aşağıdaki roller sağlanmalıdır:

8.1.4.1. Super Admin: Tüm yapıyı yönetecek en yetkili kullanıcı

8.1.4.2. Manager: Sadece kendi kurumunu yönetecek hesap türü

8.1.4.3. User: Sadece kendi kurumunda yetkisiz kullanıcı

8.1.4.4. Auditor: Sadece kampanya sonuçları, eğitim sonuçları ve istatistik! veriyi (departman bazlı grafikler, trend analizi vb.) görebilecek olan kullanıcı



- 8.1.4.5. ŞİRKET kendine özel roller tanımlayabilmeli, bu rollerin hangi modülde hangi yetkiye sahip olduğu belirlenebilmelidir.
- 8.1.5. Ürünün sunmuş olduğu raporlar XLSX, PDF, CSV veya metin formatında dışarıya aktarılabilir.
- 8.1.6. Ürün, Active Directory ile LDAP(S) protokolü aracılığıyla özel bir yetkilendirme yada sunucu sistemleri üzerine kurulum gerektirmeksizin entegre çalışmalıdır.
- 8.1.7. Ürün üzerinde yöneticilerin ve tüm kullanıcıların gerçekleştirdiği her bir işlem ve detayı (audit log) tutuluyor olmalıdır.
- 8.1.8. Active Directory ile entegrasyonlar gerçekleştirmelidir.
- 8.1.9. Uygulama multi tenant yapısını desteklemelidir.
- 8.1.10. Sisteme kayıt edilen ad,soyad ve e-posta bilgileri encrypted saklanmalıdır.
- 8.1.11. SIEM ürünleri ile entegrasyonlar gerçekleştirmelidir.
- 8.1.12. Kullanıcı grupları statik ve dinamik olarak yönetilebilmelidir.
- 8.1.13. Kurumlar platformu kendi markalarına göre özelleştirebilmelidir (White-Labeling).
- 8.1.14. Ürün internete çıkışını ŞİRKET proxy'si üzerinden yapabilmelidir.

## 8.2. OLTALAMA SİMÜLASYONU VE EĞİTİM

- 8.2.1. Ürün, kişiye özel olarak ayarlanabilir oltalama senaryolarının odağında, güncel tehditlerin benzerlerinin oluşturulması ve bu senaryolarda kurum çalışanı tehlike potansiyeline sahip bir işlem yaptığında, örneğin bir linke tıkladığında, bilgi girişi yaptığında, anlık eğitim ve geri bildirim sunacaktır.
- 8.2.2. Aşağıda yer alan simülasyon modellerini desteklemelidir;
  - 8.2.2.1. Tıklama
  - 8.2.2.2. Bilgi Girme
  - 8.2.2.3. Dosya indirme
  - 8.2.2.4. Macro çalıştırma
  - 8.2.2.5. Dosya açma
  - 8.2.2.6. Ekli dosya bilgi girişi
  - 8.2.2.7. QR Kod
  - 8.2.2.8. Combine ( Bilgi girme ve kötücül yazılım aynı model içerisinde)
- 8.2.3. Kullanıcılar için farklı senaryolarda oltalama testleri gerçekleştirmeye ve bilinç düzeyini arttıracak kampanyalar oluşturmaya olanak sağlayacaktır. Çözüm, sınırsız senaryo üretme ve rapor alma imkanına sahip olacaktır.
- 8.2.4. Ürün, hedef odaklı saldırı gerçekleştirerek hem güncel atak vektörlerini hem yaygın atak vektörlerini kullanma kapasitesine sahip olacaktır.

- 8.2.5. Sistem tarafından sağlanan hazır eposta içeriklerine ek olarak kurum tarafından kolayca eklenebilecek eposta içerikleri hızlıca ortalama kampanyalarına dönüştürülebilecektir.
- 8.2.6. Ortalama kampanyaları ile kullanıcıların farkındalığını ölçmek ve eğitmek üzere geliştirilen senaryolarda; hassas bilgi elde etme, dosya indirme ve çalıştırma gibi senaryolar kullanılacaktır.
- 8.2.7. Ek bir konfigürasyona gerek kalmadan Trusted SSL destekli ortalama URL'leri oluşturabilmelidir.
- 8.2.8. Ortalama simülasyonunda alınan parolanın güçlülük düzeyi ölçülebilmelidir.
- 8.2.9. Ortalama simülasyonunda bilgi çalma senaryosu uygulanıyorsa, parolalar veritabanına maskeli dahi olsa kaydedilmeden (on-the-fly) kurumun sağlayacağı merkezi kimlik doğrulama servisinden doğrulanarak, parolasını doğru giren veya hatalı girenler raporlanabilmelidir.
- 8.2.10. Ürün içerisindeki yalnızca tıklama, veri girişi, zararlı yazılım, web-tabanlı simülasyonlar ve usb simülasyonu gibi ortalama/sosyal mühendislik saldırısı senaryo tipleri kullanılabilir durumda olacaktır.
- 8.2.11. Ürün tek kampanyada birden fazla atak senaryosunun kullanılmasına ve ilgili atakların hedef kullanıcı kitlesine rastgele bir şekilde gönderilmesine olanak sağlayacaktır.
- 8.2.12. Belirli bir gruba gönderilecek birden fazla saldırı senaryosunun seçilmesi durumunda, saldırı senaryosu ve eğitim içeriği eşleştirmesi yapılabilir.
- 8.2.13. Çözüm atak senaryolarının gönderiminin zamana yayılarak yapılmasına olanak tanıyacaktır. Bu şekilde sistem yönetici tarafından belirlenen başlama ve bitiş tarih/saati baz alınarak, aynı kampanya için farklı kullanıcılara farklı tarih ve saatlerde gönderim yapılabilecektir. Bu özellik bir önceki maddede yer alan "tek kampanyada birden fazla atak senaryosu kullanma" özelliği ile birleştirilebilecektir.
- 8.2.14. Her kampanya sonucu detay bilgileri raporlayarak aksiyon alınmasına, kullanıcı odaklı eğitimler geliştirilmesine, kullanıcı bazlı başarı istatistik verisinin tutulmasına olanak sağlayacaktır.
- 8.2.15. Geçmiş kampanyalar, bu kampanyaların kimleri hedeflediği, başarı oranı ve gelişim süreci raporlanabilir olacaktır.
- 8.2.16. Ürünün hizmet ve raporlaması, uygulamalardan tekrarlı şekilde başarısız olan ŞİRKET çalışanlarını belirleme ve bunları rapor etme kabiliyetine sahip olacaktır. ŞİRKET için risk oluşturan kullanıcı ve grup profilleri çıkarılarak hedef odaklı eğitimler ve bilgi güvenliği politikaları oluşturmaya olanak sağlayacaktır.
- 8.2.17. Ürün, sadece sistem güncellemesi ve yeni şablonların indirilmesi için internet erişimine ihtiyaç duyacaktır. Bu işlemler için de internet erişiminin sürekli açık bırakılarak güncelleme ve yeni şablonların indirilebilmesine ŞİRKET tarafından olanak sağlanacaktır.
- 8.2.18. Ürünün sunduğu eğitim içerikleri video, infografik ve interaktif oyun dahil çeşitli

formatlarda mevcut olacaktır. Tüm eğitim içerikleri ekstra bir ücrete tabii olmadan sunulacak olup, düzenli olarak yeni eğitim içerikleri eklenecektir.

- 8.2.19. Ürün tasarlanan Oltalama ve/veya Eğitim kampanyasının başlatılmadan önce test amaçlı olarak sistem yöneticisine gönderilmesini destekleyecektir.
- 8.2.20. Ürün, sunduğu yönetim platformunda yapılan kullanıcı aktiviteleri ile ilgili detaylı olarak audit log verisi üretmelidir.
- 8.2.21. Bir üst maddede iletilen tüm audit verileri Syslog ya da DB access yöntemleriyle SIEM ürününe canlı (real-time) olarak sorunsuz alınabilmelidir.
- 8.2.22. Ürün kampanyaları aşağıdaki başlıklarda yönetebilecektir:
  - 8.2.22.1. Kampanyaları Listeleme
  - 8.2.22.2. Yeni Kampanya Oluşturma
  - 8.2.22.3. İleri Zamanlı Kampanya Oluşturma
  - 8.2.22.4. Aynı kampanyada birden fazla senaryo kullanımı
- 8.2.23. Ürün mevcut oltalama şablonlarını yönetmek ve yeni şablonlar oluşturmak için aşağıdaki ön gereksinimleri karşılayacaktır.
  - 8.2.23.1. Şablon Listeleme ve Şablonları Görsel Olarak Düzenleyebilme
  - 8.2.23.2. Yeni Şablon Oluşturma
  - 8.2.23.3. SSL Destekli Phishing URL'ler Atayabilirle
  - 8.2.23.4. Web Sitesi Kopyalama Özelliği
- 8.2.24. Ürün aşağıda belirtilen gelişmiş seçenekleri sağlayacaktır.
  - 8.2.24.1. Email Servis Ayarları
  - 8.2.24.2. LDAP Ayarları
  - 8.2.24.3. Bir kampanyada başarısız olan kullanıcılardan otomatik olarak yeni bir hedef grubu oluşturulması
  - 8.2.24.4. Ürün Adı ve Logo gibi bileşenlerin kurumun isteği doğrultusunda özelleştirilebilmesi
  - 8.2.24.5. Eğitim e-postalarının konfigure edilebilir dönemlerle kullanıcıya tekrar gönderilmesi (hatırlatıcı)
  - 8.2.24.6. Kampanyaların veya şablonların kopyalanabilmesi ve yedeklenebilmesi
- 8.2.25. Ürün rapor yönetiminde aşağıda belirtilen seçenekleri sağlayacaktır.
  - 8.2.25.1. Özet Görünüm
  - 8.2.25.2. Kampanya Adı
  - 8.2.25.3. Toplam Gönderilen E-posta Sayısı
  - 8.2.25.4. Sadece Okuyan Sayısı
  - 8.2.25.5. Tıklayan Kullanıcı Sayısı
  - 8.2.25.6. Bilgisini Giren Kullanıcı Sayısı

- 8.2.25.7. Aksiyon Göstermeyen Kullanıcılar
- 8.2.25.8. Kampanya Başlangıç Zamanı
- 8.2.25.9. Kampanyanın Bitiş Zamanı
- 8.2.25.10. Tıklayan Kullanıcı Listesi
- 8.2.25.11. Dosya İndiren Kullanıcılar
- 8.2.25.12. Zararlı Makro'yu Aktifleştiren Kullanıcı Listesi
- 8.2.25.13. Okuyan Kullanıcı Listesi
- 8.2.25.14. Bilgisini Giren Kullanıcı Listesi
- 8.2.25.15. Eposta Gönderim Raporu
- 8.2.25.16. Tam veya kısmi kullanıcı verisi toplama
- 8.2.25.17. Özel rapor şablonlarının oluşturulması
- 8.2.25.18. Şirket, Departman bazında raporlamalar
- 8.2.25.19. Geçmiş ve yeni kampanyada kampanya bazlı iyileşme miktar göstergesi
- 8.2.25.20. Eğitimlerde en çok yanlış cevap verilen sorular
- 8.2.25.21. Eğitimi tamamlama yüzdesi (kişi bazlı)
- 8.2.25.22. Tarayıcı, İP adresi ve user-agent bilgisi
- 8.2.25.23. Departmana göre ortalama/eğitim çıktısı
- 8.2.25.24. Gruba göre ortalama/eğitim çıktısı
- 8.2.25.25. Tam rapor (kullanıcı, grup, departman ortalama/eğitim bilgileri)
- 8.2.25.26. Geçmiş kampanyalar, bu kampanyaların kimleri hedeflediği, başarı oranı ve gelişim süreci raporlanabilir olacaktır.
- 8.2.25.27. Departman bazlı bütün aktivitelerin karnesini (KPI) oluşturabilecektir.
- 8.2.25.28. Çalışanların bütün aktiviteleri doğrultusunda karne (KPI) oluşturabilecektir.
- 8.2.25.29. Hedef kullanıcı bazlı aktivitelerin karnesini (KPI) oluşturabilecektir.
- 8.2.25.30. Şirket bazlı aktivitelerin karnesini (KPI) oluşturabilecektir.
- 8.2.25.31. Pozisyon, ünvan, birim, cinsiyet, yaş aralığı gibi AD üzerinde bulunan farklı kriterlere göre genel skorlar ve kampanyaya özel skorlar raporlanabilecektir.
- 8.2.26. Raporlara erişim, rol bazlı olarak kısıtlanabilecektir.
- 8.2.27. Ürün SCORM formatında hazırlanan eğitimleri içeriye alabilecek ve eğitim ataması yapabilecektir.
- 8.2.28. Ürün REST API ile üzerindeki tüm eğitim, ortalama vb. için gerekli tüm verileri servis edebilmelidir.
- 8.2.29. Ürün departmanların ortalama farkındalık istatistiğini ve eğitim istatistiğini

arayüz üzerinden gösterebilmeli, geçmişe dönük trend analizleri çıkarabilmeli ve hem arayüz üzerinden hemde rapor çıktısı olarak bu raporu sunabilmelidir.

8.2.30. Ürün; ortalama, kötücül yazılım, virüs bulaşmış bir siteye uğranıldığında kötücül yazılımların habersiz indirilmesi sonucu gerçekleşen saldırılar, sosyal medya bilgi sızdırmaları ve şüpheli eposta bildirim konularıyla ilgili olarak eğitim içeriklerini bünyesinde barındıracak bir kütüphaneye sahip olacaktır. Bu eğitim içerikleri, özelleştirilebilir html, video, infografik ve interaktif oyun dahil çeşitli formatlarda mevcut olacaktır.

8.2.30.1. Quiz soruları değiştirilebilmen, yeni sorular eklenebilmeli veya yeni bir quiz oluşturulabilmelidir.

8.2.30.2. Eğitim kütüphanesi "workshop" niteliğinde (örnek epostalar gösterilerek kullanıcının epostanın gerçek olup olmadığı konusunda karar vermesi istenerek) eğitim içerecektir.

8.2.30.3. Soru içeren eğitim veya quiz'lerin sonunda kullanıcıya başarı puanına göre soft sertifika (pdf formatında) verilebilmelidir.

8.2.30.4. Eğitimler başarılı saldırı sonrası yönlendirme ile (redirecting) veya simülasyon süresi tamamlandığı zaman eposta bildirim ile atanabilmelidir.

8.2.31. Ürün MS Active Directory (LDAP ve LDAPS entegrasyonu) ile entegre olacaktır.

8.2.31.1. AD'de grup bazında filtreleme yaparak AD Grup içeriğinin içe aktarılmasını sağlayacaktır.

8.2.31.2. Çözüm içerisinde oluşturulan kullanıcı gruplarının AD Gruplarla senkronizasyonu otomatik bir şekilde ve belirli aralıklarla yapılacaktır.

8.2.31.3. Çözüm içerisinde yer alan kullanıcı grupları için yeni tanımlayıcı alanlar (Örnek; Yaş) tanımlanarak bu alanlar Active Directory alanları (attribute) ile eşleştirilebilecektir.

8.2.31.4. AD'den yeni içe aktarılan kullanıcılar, ilgili kullanıcı grubunun bağlı bulunduğu kampanyalara otomatik olarak aktarılacak ve gerekmesi durumunda bu kullanıcılara manuel müdahale olmadan, otomatik bir şekilde eğitim ataması epostası gönderilebilecektir.

8.2.31.5. Ürün kullanıcıların ana dili bilgisine göre kampanyalarda mail gönderimi yapabilecektir. Bu bilgi LDAP üzerinde, dil bilgisini içeren herhangi bir alandan alınabilir olmalıdır.

8.2.31.6. Ürün yöneticilere/gruplara AD bilgileri ile yetkilendirme ve authentication yapabilmelidir.

8.2.32. Çalışanların eposta adresleri ve isimleri veri tabanında tutulurken AES 256 kullanılarak şifrelenecektir.

8.2.33. Ürün ikili doğrulama özelliği ile uygulamaya girişlerde ikinci bir güvenlik protokolü sunulmalıdır.

8.2.34. Ürün belirlenen tarihler arasında tüm kullanıcılara atanan eğitim bilgilerini ve

sonuçlarını tek bir sayfada raporlayabilmelidir.

- 8.2.35. Ürün; kişi, departman, grup ya da sisteme tanımlanan bütün özel bilgiler ile ortalama, eğitim, test ya da notlandırma (A,B,C,D,F) özelinde detaylı analiz/raporlama yapabilmeli, geçmişe yönelik ve şuanki durumu gösteren trend analizi çıkarabilmeli ve gerçekleştirdiği analizler sonucunda tespit edilen kullanıcılara özel yeni bir çalışma grubu oluşturma ya da belirli bir gruba kayıt etme yeteneğine sahip olmalıdır.
- 8.2.36. Ürün 4.2.35 başlığında belirtilen raporlamayı belirlenen kullanıcılara, belirlenen periyotlarda rapor olarak gönderebilmelidir. Grup ve departman bazında yöneticilere otomatik bildirimler yapabilmelidir.
- 8.2.37. Ortalama, eğitim, test ya da notlandırma özelinde belirli bir tarih aralığında notu düşen/artan kullanıcılar özelinde detaylı analiz/raporlama yapabilmeli ve gerçekleştirdiği analizler sonucunda tespit edilen kullanıcılara özel yeni bir çalışma grubu oluşturma ya da belirli bir gruba kayıt etme yeteneğine sahip olmalıdır.
- 8.2.38. Ürün bilgi güvenliği başlıklarında en çok hangi konularda personelin başarısız olduğunu tek bir ekranda istenirse departman bazlı, istenirse kurum geneli bazında raporlama ve arayüz üzerinden de göstererek kurumun aksiyon almasına yardımcı olmalıdır.
- 8.2.39. Ürün tek parça olarak DMZ üzerinde konumlandırılması yerine, 2 parça halinde (DMZ üzerinde reverse proxy + LAN üzerinde main server) çalışabilirdir.
- 8.2.40. Yönetim ekranına erişim https protokolü üzerinden olmalıdır.
- 8.2.41. Ürün, simülasyon amaçlı yapılan saldırı testleri web tabanlı merkezi yönetim bileşeni üzerinden yönetilebilecek ve raporlanabilecektir.
- 8.2.42. Bir kampanyada başarısız olan ( «oltaya gelen») kullanıcılar tek tıkla yeni ve boş bir gruba aktarılabilir.
- 8.2.43. Yeni eğitimlerin ve şablonların indirilmesi ürün web arayüzünden basit tıklama işlemleri ile kolayca yapılabilecektir. Eklenen yeni içeriklerin istatistiği arayüz üzerinden görüntülenebilmelidir. (Ör: ŞİRKET tarafından belirlenen tarih aralığında kaç adet yeni içerik eklendiği)
- 8.2.44. Ürün REST API özelliğini sunacaktır. Arayüzden yapılabilecek tüm işlemler ve raporlama için ihtiyaç duyulabilecek tüm verilerin çekilmesi işlemi, REST API üzerinden de yapılabilir olacaktır.
- 8.2.45. Eğitim modülü eğitimi destekleyecek aşağıdaki materyalleri sunmalıdır:
- 8.2.45.1. Haftalık Bültenler
  - 8.2.45.2. Posterler
  - 8.2.45.3. İpucu ve önerileri
  - 8.2.45.4. Anketler
  - 8.2.45.5. Sınavlar

#### 8.2.45.6. Ekran koruyucular

- 8.2.46. Ürün çalışanların bütün aktiviteleri bağlamında karne (KPI) oluşturabilmelidir.
- 8.2.47. Departman bazlı bütün aktivitelerin karnesini(KPI) oluşturulabilmelidir.
- 8.2.48. Hedef kullanıcı bazlı aktivitelerin karnesini (KPI) oluşturulabilmelidir.
- 8.2.49. Şirket bazlı aktivitelerin karnesini (KPI) oluşturulabilmelidir.
- 8.2.50. Bütün aktivitelerin listesi ham veri olarak indirilebilmelidir.
- 8.2.51. Ürün ŞİRKET'in ihtiyacı dahilinde özelleştirebilir rapor şablonları sunabilmelidir. Bu rapor şablonları arayüz üzerinden düzenlenebilmelidir.
- 8.2.52. Ürün platforma kayıtlı tüm alt şirketlerin (iştirak) listesi raporlanabilmelidir. Üründe sunulan tüm raporlama özellikleri alt şirketler bazında da yapılabilmelidir.
- 8.2.53. Ürün politika yönetimi için altyapı sunmalıdır. Kurumun belirlediği politikayı, belirli kullanıcı gruplarına ileterek onay alabilmeli ve raporlayabilmelidir.
- 8.2.54. Politika onayının önüne ya da arkasına eğitim eklenebilmelidir.

### 8.3. ŞÜPHELİ E-POSTA RAPORLAMA EKLENTİSİ

- 8.3.1. Çalışanlar tek bir tıklamayla şüpheli e-postayı rapor edebilmelidir.
- 8.3.2. Kullanıcılardan erken ortalama uyarıları alınarak proaktif bir sensör ağı oluşturulmalıdır.
- 8.3.3. Kullanıcı, simüle edilmiş bir ortalama güvenlik testinde "Ortalama Raporla" butonunu tıkladığında, kullanıcının bu doğru eylemi raporlanabilmelidir.
- 8.3.4. Ortalama bildirme işlemini Outlook masaüstü, mobil ve web uygulamalarında yapılabilirliği açıklanmalıdır. Tüm uygulamalarda bu özelliğin çalışması tercih sebebidir. YÜKLENİCİ' eksik durumlarda gereken entegrasyonun geliştirilebilirliği geliştirilemeyeceğini açıklamalıdır.
- 8.3.5. Çalışanlar, eğitimlerini güçlendiren anında geri bildirimler alabilmelidir.
- 8.3.6. Proxy desteği olmalıdır.
- 8.3.7. On-premise, cloud ve hybrid olarak çalışabilmelidir.
- 8.3.8. Şüpheli e-posta analiz eklentisinin kimlerde kurulu olduğu ve kaç kişide aktif olarak kullanıldığı ve eklenti sürüm bilgisi arayüzden tespit edilebilmelidir.
- 8.3.9. Şüpheli e-posta raporlama eklentisi Office365, Exchange, OWA, Outlook Mobil ve Windows Outlook (2016 ve üstü) sürümlerini desteklemelidir.
- 8.3.10. Şüpheli e-posta'lar IOS ve Android mobil cihazlardan da raporlanabilir olmalıdır. Bunun için kurumun mail altyapısı desteklemelidir.
- 8.3.11. Şüpheli e-posta gönderme eklentisi birden fazla dili desteklemelidir. Bu diller ve içerisindeki mesajlar plugin oluştururken özelleştirilebilmeli, her bir dilin gösterdiği mesaj yönetim paneli üzerinden değiştirilebilir olmalıdır.
- 8.3.12. Eklenti kullanıcının Outlook dil tercihini baz alarak gösterdiği metinleri bu dilde



gösterebilmelidir.

8.3.13. Şüpheli e-posta raporlama eklentisi ürünün arayüzünden özelleştirilebilmeli ve bu değişikliklerin uygulaması için yeni bir eklenti dağıtılmamalı. Bunlar:

- 8.3.13.1. Eklenti logosu
- 8.3.13.2. Eklenti adı
- 8.3.13.3. Eklentinin marka adı
- 8.3.13.4. Şüpheli e-postanın gönderileceği adres
- 8.3.13.5. Çoklu Dil Destekli Şüpheli e-postanın bildirim konusu
- 8.3.13.6. Çoklu Dil Destekli Şüpheli e-postanın bildirim iletisi
- 8.3.13.7. Çoklu Dil Destekli Şüpheli e-postanın silme iletisi
- 8.3.13.8. Çoklu Dil Destekli Şüpheli e-postanın teşekkür mesajı
- 8.3.13.9. Çoklu Dil Destekli Şüpheli e-postanın uyarı mesajı

## 9. İşin İfası ile İlgili Şartlar (YÜKLENİCİ Sorumlulukları)

### 9.1. KURULUM VE KONFIGÜRASYON

- 9.1.1. Teklif edilen tüm ürünlerin kurulumu, üreticinin ya da yüklenicinin konusunda sertifikalı uzmanları tarafından yapılacaktır.
- 9.1.2. Yüklenici, teklif edilen ürünlerin kurulumundan ve çalıştırılmasından sorumludur.
- 9.1.3. Garanti süresi ve ücretli bakım-onarım dönemlerinde gerçekleştirilecek yazılım sürüm değişiklikleri ile ilgili olarak; her bir yeni sürüm için, Şirket ve Yüklenicinin karşılıklı mutabakatı ile belirlenen tarihte yeni sürüm güncellemesini Yüklenici gerçekleştirecektir.
- 9.1.4. Yüklenici, teklif edilen ürünlerin tamamının, garanti süresi içindeki tüm bakım, onarım, destek, sürüm yenileme işlemlerinden sorumludur.
- 9.1.5. Teklif edilen ürünlerin kurulumları ŞİRKET'İN belirleyeceği zamanlarda ve lokasyonlarda yapılacaktır. Belirlenen zaman mesai saatleri dışında ve hafta sonu olabilecektir. Yüklenici bu hizmet için ekstra ücret talep etmeyecektir.
- 9.1.6. Tüm bu kurulumlar için yüklenici; ilave hizmet, ulaşım, konaklama gibi ücretler talep etmeyecektir.
- 9.1.7. Yüklenici, kurduğu sistemlerin kuruluşlarından kaynaklanan problemler sebebi ile yapılacak müdahalelerin, garanti kapsamı içerisinde değerlendirilecektir.
- 9.1.8. Kurulum sonrası kontroller Şirket teknik personeli tarafından yapılacaktır. İlgili tutanaklar düzenlenecektir.

### 9.2. PROJE YÖNETİMİ

- 9.2.1. Sözleşmenin imzalanmasını müteakip başlayacak proje yönetimi, Şirket ve Yüklenici tarafından bir arada yürütülecektir.
- 9.2.2. Projenin merkezi yönetimi Şirket'te olacaktır.
- 9.2.3. Projede takip edilmesi gereken proje adımlarına uygun bilgi, eğitim ve gerekli kaynaklar Yüklenici tarafından sunulacaktır.

9.2.4. Ana Alımlar Kapsamında satın alınacak ürünlerin, entegrasyonu, uyarlaması ve çalışır hale getirilmesine yönelik yapılacak proje, teknik şartnamede belirtilen süreler içerisinde tamamlanacaktır.

9.2.5. Teslimat ile ilgili teslimat planı, işbu şartnameye verilecek cevaplar ile birlikte Firma tarafından teslim edilecek ve sözleşme imzalandıktan sonra yapılacak işler bu takvime uygun olarak gerçekleştirilecektir.

### 9.3. PROJE DEĞİŞİKLİK YÖNETİMİ

9.3.1. Proje Değişiklik Yönetimi Prosedürü; Yüklenici ve Şirket'in karşılıklı mutabakatıyla oluşacak proje planı içerisinde yer almayan, kullanıcı kabul testlerinde bildirilmemiş değişiklikler ya da kesin kabul sonrasında talep edilecek değişiklikler için uygulanacaktır.

9.3.2. Bu tür değişiklikler, PDİF ile değişikliğin gerekçesi açıklanarak Şirket Proje Yöneticisi aracılığı ile Yüklenici Proje Yöneticisine iletilecektir.

9.3.3. Yüklenici proje yöneticisi talebi gözden geçirip, daha detaylı araştırma için kabul edecek ya da reddedecektir. Detaylı araştırmanın (talep) Yüklenici Proje Yöneticisi tarafından kabul edilmesi durumunda, Şirket ve Yüklenici Proje Yöneticileri PDİF' yi imzalayacak ve bu işin siparişi anlamına gelecektir. Firma Proje Yöneticisi tarafından reddedilmesi durumunda ise Firma Proje Yöneticisi reddetme gerekçelerini detaylı olarak PDF üzerinde açıklayacaktır. Firma reddetme gerekçesinin ŞİRKET tarafından onaylanması gereklidir.

9.3.4. Araştırma konusu olan değişikliklerin uygulanabilmesi için ŞİRKET tarafından Proje Yöneticisinin, Firma tarafından Proje Yöneticisi ve Danışman/Danışmanların yazılı Değişiklik Onayını ve/veya Proje Değişiklik İstek Formu'nu (PDİF) imzalaması gerekir.

### 9.4. İŞ SÜREKLİLİĞİ GEREKSİNİMLERİ

9.4.1. Değişim ve entegrasyon herhangi bir hizmet kesintisine neden olmayacak şekilde planlanacak ve gerçekleştirilecektir.

9.4.2. Mevcut altyapıda kesintisiz değişim; yaygınlaştırma ve entegrasyon planları ile gerçekleştirilecek ve takip edilecektir.

9.4.3. Şirket'in iş sürekliliğini ve satın alınan Platformun kesintisiz olarak hizmet vermesini sağlamak için; satın alınan Platform ile ilgili olarak Yüklenici tarafından iş sürekliliği ve acil durum planları ve destekleyici çalışmalar (iş etki analizi, risk analizi, iş süreklilik ve acil durum dokümantasyonu, yedekleme planları vb.) yapılacaktır.

9.4.4. Şirket'in iş sürekliliğinin sağlanmasına destek olmak üzere Şirket tarafından talep edilen durumlarda; Yüklenici bu sözleşme kapsamında sağlanacağı belirtilen servis seviyelerine uygun şekilde gerekli desteği Şirket'in bildiriminden itibaren istenilen lokasyon için sağlayacaktır.

9.4.5. Hardware maintenance, firmware upgrade, hardware upgrade gibi işlemleri kesintisiz olarak gerçekleştirilebilecektir.

### 9.5. DOKÜMANTASYON VE SERTİFİKALAR

9.5.1. Yüklenici, teklif ettiği tüm yazılım ve donanım bileşenlerine ilişkin orijinal belge, sertifika, kullanım kılavuzu, sürücü yazılımı, elektronik ortamda orijinal şekilde Şirket'e teslim edecektir.

9.5.2. Yüklenici teklif edilen ürün(ler) ile ilgili olarak detaylı teknik dokümantasyonu Şirket tercihi doğrultusunda Türkçe ve/veya İngilizce olarak sağlayacaktır.

9.5.3. Yüklenici, ürünlerin kullanım kılavuzlarını ve işletim sürecinde gerekli olabilecek tüm destek dokümanlarını 1'er (bire) adet elektronik ortamda ve Şirket tarafından gerekli görülür ise 1'er (bire) adet basılı olarak Şirket'e teslim edecektir.



- 9.5.4. Kesin kabul işleminden sonra uygulama ile ilgili yapılan/yapılacak güncelleme ve sürüm değişikliklerinden oluşan/değişen dokümanlar her seferinde elektronik ortamda Şirket'e teslim edilecektir.
- 9.5.5. Teslim edilecek tüm donanım birimleri tamamen yeni ve hiç kullanılmamış olacaktır.

## 9.6. BİLGİ GÜVENLİĞİ GEREKSİNİMLERİ

- 9.6.1. Yüklenici, teklif vermekle, ihale evrakları arasında yer alan Gizlilik Taahhütnamesi'ni imzalamayı ve bu taahhütnamede yer alan hususlara uymayı peşinen kabul etmiş sayılacaktır.
- 9.6.2. Hem ürünün kendisi, hem uygulama süresince Yüklenicinin yürüteceği çalışmalar, Şirket'i güvenlik açıklarına maruz kalmasına neden olmayacaktır.
- 9.6.3. Yüklenici kodlarının statik kaynak kod analiz raporunu Şirket'e sağlamalıdır.
- 9.6.4. İşletim sistemi ve veritabanı yönetim sistemlerinde var olan veya çıkabilecek güvenlik yamaları için yapılacak testler esnasında Yükleniciden destek talep edilmesi durumunda Yüklenici ek bir ücret talep etmeksizin uygulama testleri için destek verecektir.
- 9.6.5. Konsol üzerinden erişimler kullanıcı adı ve parolasıyla kısıtlanabilecektir.
- 9.6.6. Yüklenicinin Şirket sistemlerine uzaktan erişimi gerekmesi halinde, Şirket bilgi güvenliği politika ve standartları geçerli olacaktır. Bu kapsamda yüklenici aşağıdaki koşulların sağlanması halinde sadece geliştirme ve test ortamlarına erişim izni sağlanabilecektir.
- 9.6.6.1. İlgili geliştirme ve test ortamının izole bir ağ segmentinde bulunması,
- 9.6.6.2. İlgili geliştirme ve test ortamında herhangi bir üretim ortamı verisi bulunmaması,
- 9.6.6.3. İlgili geliştirme ve test ortamına erişimler terminal sunucu üzerinden gerçekleştirilmesi ve yapılan işlemlerin kaydedilmesi.
- 9.6.7. Firma, ŞİRKET lokasyonunda çalışırken geliştirme ve test ortamlarına bağlanmak için ŞİRKET tarafından sağlanan domaine (MS AD) kayıtlı bilgisayarı ile çalışmasını yapacaktır. Geliştirme (development) ve test ortamlarına uzaktan erişim sağlanabilir fakat bu ortamlar kesinlikle üretim ortamı verisi içeremezler ve üretim ortamına doğrudan ya da uygulama katmanından erişemezler.
- 9.6.8. Garanti süresi boyunca, canlı ortamda tespit edilecek güvenlik bulguları da Yüklenici tarafından ücretsiz olarak kapatılacaktır.
- 9.6.9. Yönetim amaçlı yapılan işlemler loglanabilecektir.
- 9.6.10. Yüklenici bilgi güvenliğinin sağlanabilmesi için Şirket tarafında uygulanan politika, kurallar ve standartlara uygun davranacaktır.
- 9.6.11. Yüklenici Uygulama için bulunan/alınan güvenlik sertifikalarını/kriterlerini teklifine ekleyecektir/belirtecektir.

## 10. Eğitim

- 10.1. Yüklenici, ilgili ürünlere ilişkin olarak kullanım ve işleme yönelik teknik eğitimlerini verecektir.
- 10.2. Yüklenici, eğitimleri teklif edeceği ekipmanlar ile uygulamalı olarak verecektir.
- 10.3. Eğitimler, ürünün teknik yönetimi, kullanımı ve varsa script dili öğrenimini içerecektir.
- 10.4. Yüklenici, eğitimler sırasında destek amaçlı olarak kullanılacak eğitim dokümanlarını ŞİRKET'E sağlayacaktır.



- 10.5.** Tüm eğitimler, Şirket tarafından talep edilmesi durumunda mesai saatleri dışında verilebilecek şekilde planlanacaktır.
- 10.6.** Ürünlere ilişkin en az 3 (üç) tam mesai günü süresince yapılacak ve kişi sınırı bulunmayacaktır.
- 10.7.** Tüm eğitimler, YÜKLENİCİ'NİN üretici tarafından sertifikalandırılmış yetkili eğitimleri tarafından verilecektir.
- 10.8.** Yüklenici tarafından verilen eğitimlerin yetersiz veya başarısız bulunması durumunda başarısız eğitimler ücretsiz tekrarlanacaktır.

## 11. Lisanslar

750 Kullanıcı lisansı olmalıdır.

## 12. Raporlama

### 12.1. ÖLTAAMA SİMÜLASYONU

12.1.1. Öltalama simülasyonu kampanyası ile minimum aşağıdaki çıktılar raporlanabilmelidir,

12.1.1.1. Toplam Gönderilen E-posta Sayısı

12.1.1.2. Sadece Okuyan Sayısı

12.1.1.3. Tıklayan Kullanıcı Sayısı

12.1.1.4. Bilgisini Giren Kullanıcı Sayısı

12.1.1.5. Aksiyon Göstermeyen Kullanıcılar

12.1.1.6. Farklı kullanıcıların öltalama detayları kıyaslanmalıdır.

12.1.1.7. Kampanya Başlangıç Zamanı

12.1.1.8. Kampanyanın Bitiş Zamanı

12.1.1.9. Öltalama raporundaki tüm kullanıcılara öltalama emaillerin toplamda ne kadar sürede gönderildiği

12.1.1.10. Rapor İstatistikleri

12.1.1.10.1. Okumada Kullanılan İnternet Tarayıcıları

12.1.1.10.2. Tıklayan Kullanıcılar

12.1.1.10.3. Okuyan Kullanıcılar

12.1.1.10.4. Simülasyonu Raporlayan Kullanıcılar

12.1.1.10.5. Bilgisini Giren Kullanıcılar

12.1.1.10.6. Eposta Gönderim Raporu

12.1.1.10.7. Tarayıcı, lokasyon, IP adresi ve user-agent bilgisi

12.1.1.10.8. Departmana göre öltalama çıktısı olmalıdır

12.1.1.10.9. Tam rapor indirilebilmelidir.

12.1.1.10.10. Rapor çıktısı grafikler üzerinde gösterilebilmelidir



12.1.1.10.11. Rapor çıktısına göre ilgili ortalama kampanyası tek tıkla tekrar istenen hedefe gönderilebilmelidir.

12.1.1.10.12. Ortalama simülasyonuna tepki vermeyenler raporlanmalıdır.

12.1.1.10.13. E-posta'yı şüpheli olarak raporlayan kullanıcıya ait bilgiler gösterilmelidir.

## 12.2. ONLİNE EĞİTİM

12.2.1. Eğitim sonuçlarının raporlanması minimum aşağıdaki gereksinimleri sağlamalıdır,

12.2.1.1. Toplam eğitim atanan kullanıcı sayısı

12.2.1.2. Eğitim e-postasının ulaştığı kullanıcı sayısı ve detayı

12.2.1.3. Eğitim e-postasını açan kullanıcı sayısı ve detayı

12.2.1.4. Eğitim linkini tıklayan ve eğitime kullanıcı sayısı, detayı

12.2.1.5. Eğitimde var olan sınavı çözen kullanıcıların sayısı ve detayı

12.2.1.6. Sınavdan geçen ve kalan kullanıcıların sayısı ve detayı

12.2.1.7. Sınav skor tablosunu ve kullanıcı detayı

12.2.1.8. Eğitimin tamamlanma yüzdesi ve detayları

12.2.1.9. Kişi, departman ve Şirket(ler) bazında eğitimlerdeki ilerleme raporu

## 12.3. GELİŞMİŞ RAPORLAMA

12.3.1. Çalışanların bütün aktiviteleri bağlamında karne (KPI) oluşturabilmelidir.

12.3.2. Departman bazlı bütün aktivitelerin karnesini(KPI) oluşturabilmelidir.

12.3.3. Hedef kullanıcı bazlı aktivitelerin karnesini (KPI) oluşturulabilmelidir.

12.3.4. Şirket bazlı aktivitelerin karnesini (KPI) oluşturulabilmelidir.

12.3.5. İlgili kurumun farkındalık platformuna erişim durumları arayüzden raporlanabilmelidir. (Analytics, Statistics)

12.3.6. İlgili Şirket'in farkındalık platformuna kayıtlı bütün kullanıcı listesi raporlanabilmelidir.

12.3.7. İlgili Şirket'in farkındalık platformuna kayıtlı bütün alt şirketlerinin listesi raporlanabilmelidir.

12.3.8. İlgili Şirket farkındalık platformu üzerindeki hazır raporları kullanabilmelidir.

12.3.9. İlgili Şirket kullanıcılarının eğitimleri alma durumlarını, farkındalık ilerleyişlerini, liderlik sıralamalarını görüntüleyebilmelidir.

## 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

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



### 13.2. Bakım

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

### 13.3. Kesin kabul

Kesin kabul kurulumların tamamlanması Şirket tarafından ürünün sağlıklı çalıştığının onaylanması ile gerçekleşecektir.

## 14. Birim Fiyatlar ve Birim Fiyat Tarifeleri

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

Sözleşmeye konu olan işe ilişkin gerekli makine, ekipman, işyerleri, malzemeler ve çalışanların teminini sağlamakla YÜKLENİCİ sorumludur.

## 16. Teklif Fiyatına Dahil Olan/Olmayan Hususlar

### 17. Teslimat

### 18. Fiyat Farkları ile İlgili Hususlar

### 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 almak,
- 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 özellikleri 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.