

TÜRKİYE ŞEKER FABRİKALARI A.Ş.
GENEL MÜDÜRLÜK VE FABRİKA BİRİMLERİNDE KULLANILMAKTA OLAN
BİLİŞİM ÜRÜNLERİ PARÇALI BAKIM, ONARIM VE NETWORK AĞ GÜVENLİĞİ HİZMETİNE
İLİŞKİN TEKNİK ŞARTNAME

1. KONU

Genel Müdürlüğümüz ile **Ağrı, Ankara, Burdur, Elazığ, Erciş, Ereğli, Eskişehir, Iğın, Kars, Kastamonu, Malatya, Susurluk, Uşak, Yozgat Şeker Fabrikaları, Ankara, Eskişehir Makine Fabrikaları, Ankara EMAF ve Ankara Şeker Enstitüsü** Müdürlüklerinde bulunan ve aşağıdaki tabloda belirtilen Bilişim ürünleri parçalı bakım, onarım hizmeti ile Türkşeker Bilişim Sistemleri ve Network ağ güvenliğinin sağlanması için güvenlik ürünlerinin yenilenmesi/güncellenmesi hizmetinin sağlanması işidir.

2. AMAÇ

- 2.1.** İDARE’de bulunan Network ürünleri ve yan donanımlarının parçalı bakım ve onarımlarının yapılması,
- 2.2.** İDARE’de bulunan güvenlik ürünlerinin kullanımına, güncellenmesine ve bakım onarımına yönelik satın alınacak hizmet ve ürünler ile İDARE’nin bilişim sistemlerinde güvenliğin ve sürekliliğinin sağlanması.
- 2.3.** Bu ürünlerin en etkin şekilde güvenliği sağlayabilmeleri, en son tehditlere karşı İDARE kullanıcı ve sunucularını koruyabilmesi ve en son yazılım versiyonlarıyla etkinliklerini artırabilmeleri için üretici firmalardan geçerli lisanslı ürünlerin İDARE’de bulunmasının sağlanması.
- 2.4.** Bakım kapsamındaki tüm donanım ve yazılım ürünleri ile ilgili uzman personelden teknik destek alınmasının sağlanması.

3. KISALTMALAR

İDARE/KURUM	Türkiye Şeker Fabrikaları A.Ş. Genel Müdürlüğü
İSTEKLİ	İhaleye teklif veren firma
YÜKLENİCİ	Bu şartnamede belirtilen işi alan firma
TARAF	İDARE veya YÜKLENİCİ
ÜRETİCİ FİRMA	Bu şartname kapsamı ürünleri üreten firma
ÜRÜN	İhale kapsamında teklif edilen her türlü malzeme, cihaz
PARÇALI BAKIM	Bu şartname kapsamında belirtilen donanım ve yazılımların tanımlanmış görevlerini veya fonksiyonlardan bir veya birkaçını yerine getirmemesi durumunda sistem bileşenlerinden bir veya birkaçını ya da sistemin tamamını değiştirmeyi de kapsayan arızanın giderilmesi işlemi
SİSTEM	İhale kapsamında kullanılan her türlü malzeme ve hizmetlerin bütünü
MS	Microsoft
TEKNİK ŞARTNAME	İşbu teknik şartname ve tüm ekleridir.
ŞÖZLEŞME	Tekliflerinin değerlendirilmesi sonucu, ihaleyi kazanan Firma ile İdare arasında imzalanacak olan sözleşme.
NGFW	Yeni Nesil Güvenlik Duvarı
SIEM	Güvenlik Bilgileri ve Olay Yönetimi (Security Information and Event Management)

MÜDAHALE	Sorunun başlama zamanından itibaren, sorunun çözümüne ilişkin çalışmaların YÜKLENİCİ tarafından başlatılması
ÇÖZÜMLEME	İdare tarafından cihaz sorun bildiriminden itibaren, sorunun çözülmesi ve hizmet işlemine başlaması
KABUL İŞLEMİ	Yüklenici tarafından iş bu şartname maddelerine uygun olarak şartların tamamlanması, idarenin Komisyonu tarafından yapılacak kontroller ile onaylanmasıdır.
HİZMET İŞLEMİ	Cihazların veri kaybına yol açmadan aktif çalışır bir şekilde bağlı bulunduğu sunuculardaki/sistemlerdeki işlemleri gerçekleştirmesidir

4. KAPSAM

4.1. İDARE'nin bünyesinde bulunan ürünler Genel Müdürlük ve Taşra Teşkilatında yer almaktadır. Her türlü bakım ve destek yerinde yapılacaktır. Kısmi teklif mevcut olup şu şekilde yapılabilir:

4.1.1. Aşağıda 4.2 maddesinde açıklanan 1.Kısım ürünlerine (**Tablo 1.1 ve Tablo 1.2**) birlikte tek bir teklif olarak verilecektir.

4.1.2. 2.Kısım **Tablo 2** ürünleri, 3. Kısım **Tablo 3** ürünlerini içermekte olup tablo bazlı kısmi teklife açıktır.

4.2. 1.KISIM: Bilişim Sistemlerini oluşturan **Tablo 1.1**; Sunucu, Switch, Modem, Network ürünlerinin parçalı bakım ve onarım işi olup, ücretleri bakım yapılan ayın sonunda, aylık olarak ödenecektir. **Tablo 1.2**; Veri Depolama Ürünlerinin Teknik Destek ve Güncelleme teklifi verilecek olup, bu ürünlere ait ödemeler, lisans güncellemeleri yapıp, ilgili versiyonların kurulumu yapıldıktan sonra Yüklenicinin keseceği faturaya istinaden cari usullerimize göre tek seferde ödenir.

4.3. 2.KISIM: Bilişim Sistemlerini oluşturan **Tablo 2**; Masaüstü Antivirüs Teknik Destek ve Güncelleme (SESC+DLP Lisansları), Antispam Filtreleme Teknik Destek ve Güncelleme, Anti Malware / İçerik Tarama ve Sandboxing Teknik Destek ve Güncelleme Hizmetlerini kapsar. Söz konusu ürünlerin lisans güncellemeleri yapıp, ilgili versiyonların kurulumu tamamlandıktan sonra Yüklenicinin keseceği faturaya istinaden cari usullerimize göre tek seferde ödenir.

4.4. 3. KISIM: Bilişim Sistemlerini oluşturan **Tablo 3**; Şirketimizde kullanılmakta olan Güvenlik Duvarı ve LOG Toplama Sistemlerinin Yenileme, kurulum, teknik destek, bakım, eğitim ve danışmanlık hizmetleri ile WEB Koruma Yazılımı (FortiWeb WAF) Teknik Destek ve Güncelleme Hizmetini kapsamaktadır. Bu ürünlere ait ödemeler, söz konusu ürünlerin kurulumlarının tamamlanıp aktif olarak kullanılmaya başlanmasından sonra Yüklenicinin keseceği faturaya istinaden cari usullerimize göre tek seferde ödenir.

5. MEVCUT YAPI

5.1. İDARE'nin Bilişim merkezi Ankara'da bulunan Genel Müdürlük binasındadır. İDARE Genel Müdürlük ve 14 Şeker Fabrikası, 2 Makine, 1 Elektro Mekanik Aygıtlar Fabrikası, 1 Şeker Enstitüsü Müdürlüğünden oluşmaktadır. Online çalışan uygulamalar dışında, Merkezle data

transferleri tarafımızca belirlenen zaman aralıklarına göre replikasyonla sağlanmakta, Merkez (Genel Müdürlük) verisi Eskişehir FKM'ye replike edilmektedir.

5.2. İstekliler, bilişim altyapımızın detayı hakkında daha fazla bilgiye ihtiyaç duyarlarsa, Bilgi Teknolojileri Dairesi Başkanlığından her türlü bilgiyi bizzat başvurarak alabilirler.

6. GENEL MÜDÜRLÜK VE FABRİKALARIMIZDA BULUNAN ÜRÜN LİSTESİ

Ürünün Bulunduğu Birim	Veri Dep. IBM V7000-V7200	Dell PE R900 + R620	Dell PE R730 Sunucu	DELL R440 Sunucu	FIJITSU RX300 S6	LENOVO SR 650	HP 24+48 Port Switch	Juniper 4200(4)+22	Huawei 12+24+48	SAN Switch (2) +
Genel Müdürlük	2	2	4	1	1	3	16	5	2	2
Ağrı Şeker Fabrikası				1	1		3		3	
Ankara Şeker Fabrikası				1	1		4		8	
Ankara Makine Fabrikası				1	1		2		3	
Burdur Şeker Fabrikası				1	1		2		3	
Elazığ Şeker Fabrikası				1	1		3		2	
EMAF				1	1		3		4	
Erciş Şeker Fabrikası				1	1		3		4	
Ereğli Şeker Fabrikası				1	1				4	
Eskişehir Şeker Fabrikası				1	1		3		5	
Eskişehir Makine Fab.				1	1		2		12	
İlgın Şeker Fabrikası				1	1		3		3	
Kars Şeker Fabrikası				1	1		3		3	
Kastamonu Şeker Fab.				1	1		4		5	
Malatya Şeker Fabrikası				1	1		4		5	
Susurluk Şeker Fabrikası				1	1		4		5	
Şeker Enstitüsü Müd.				1	1		12		7	
Uşak Şeker Fabrikası				1	1		4		4	
Yozgat Şeker Fabrikası				1	1		2		3	
TOPLAM	2	2	4	19	19	3	77	5	85	2

7. İŞLETİM SİSTEMLERİ VE YAZILIMLAR

- 7.1.** Genel Müdürlük ve tüm fabrikalarda bakım hizmeti verilecek ürünler üzerinde; Windows 2008 R2, 2012, 2016, 2019, 2022 Server işletim sistemleri, SQL Server 2008 R2, 2016 ve 2019 veri tabanı, Vmware sanallaştırma çözümü, Exchange 2019 ve İDARE tarafından geliştirilen Uygulama Programları ile Elektronik Belge ve Doküman Yönetim Sistemi (EBYS) ile Coğrafi Bilgi Sistemi (CBS), Uydudan Ekim Alanlarının Takibi (PTS), Personel Devam Kontrol Sistemi (PDKS), Kurumsal Kaynak Planlama Bilgi Sistemi (KKPBS) uygulamaları çalışmaktadır.
- 7.2.** 6.Madde’de bahsi geçen ürünlerde ortaya çıkan arızalar Yüklenici tarafından arıza giderme süresi dahilinde giderilecektir. Bir üründe ortaya çıkan arıza, yama ya da yeni sürümün uygulanmasını gerektirir ise İDARE ile görüşülecek ve çözüm için birlikte karar verilecektir.

8. ANTIVIRUS/ANTISPAM, OLAY MÜDAHALE GÜVENLİK YAZILIMLARI, İÇERİK TARAMA VE BİLGİSAYAR GÜVENLİĞİ TEKNİK DESTEK ve GÜNCELLEME HİZMETİ

- 8.1.** İDARE’imizde kullanılmakta olan 1000 kullanıcı lisanslı Symantec Mail Security for SMTP Antispam ürününün 1(bir) yıl süre ile güncellemesi yapılacaktır.
- 8.2.** İDARE’imizde kullanılmakta olan 1200 kullanıcı lisanslı Symantec Antivirüs Enterprise Edition ürününün Symantec Endpoint Security Complete SESC+DLP Lisansları şeklinde 1 (bir) yıl süre ile güncellemesi yapılacaktır. Kullanıcı makinelerinde yüklü olan Antivirüs yazılımlarının güncel sürüme (versiyon) yükseltilmesi, EDR ve DLP için yeni versiyonların testi, dağıtımı ve kurulumu yapılacaktır.
- 8.3.** İDARE’nin kullandığı Anti Malware / İçerik Tarama ve (Sandboxing) Bilgisayar Güvenliği ürününün 1 (bir) yıllık teknik destek ve güncelleme hizmeti alınacaktır.
- 8.4.** Mail Gateway tarafında güncelleme ve politika kontrolleri ve kurum ihtiyacına göre sıkılaştırmalar yapılacaktır.
- 8.5.** Malware Analysis ürünü için imaj hazırlama işlemleri, CAS ürün desteği sağlanacaktır.
- 8.6.** Yüklenici, bakım ve destek hizmetini çözemediği bir sorun olduğunda, üretici veya Türkiye dağıtıcısından destek alacaktır.
- 8.7.** Yüklenici, Bilişim ürünleri parçalı bakım, onarım ve network ağ güvenliği hizmetleri sözleşmesinin yürürlüğü süresince, bünyesinde gerekli görülen durumlarda ileri seviye sorunların çözümü için aşağıdaki belgelere sahip uzmanlarla destek sağlayacaktır. Bu ekipte yer alacak olan personelde aşağıdaki sertifikalar bulunacak olup, sözleşmeyi müteakip İDARE’ye sunacaktır.
- 8.7.1.** En az 1 (bir) adet Broadcom Technical Specialist sertifikasına sahip uzman.

9. LOG YÖNETİMİ SİSTEMİ ve SIEM (Güvenlik Bilgileri ve Olay Yönetimi) Yazılımı

9.1. Log Yönetimi Sistemi Konu ve Kapsam

İDARE bünyesindeki bilişim tabanlı hizmetlerin güvenliğini ve sürekliliğini sağlamak adına Log Yönetimi Sistemi ve SIEM (Güvenlik Bilgileri ve Olay Yönetimi) Yazılımı temin edilmesini kapsar.

9.2. Log Yönetimi Sistemi Genel Hususlar

- 9.2.1. Yüklenici, bu teknik şartname kapsamında aşağıda teknik özellikleri belirtilen ürünler için sözleşme tarihinden itibaren geçerli olmak üzere 3 (üç) yıl süre ile lisans temini, teknik destek bakım ve garanti hizmeti işini teklif edecektir.
- 9.2.2. İşin tamamlanma süresi Yüklenici sözleşme imzalandıktan sonra 60 gündür.
- 9.2.3. Mevcut ürünlerin içerisinde üretimden kalkmış (End Of Life) ve End Of Sale duyurusu yapılmış ürünler kesinlikle önerilmeyecektir. Bu ürünler yerine en az aynı teknik özellikler sağlanmak kaydıyla daha üst özelliklere sahip ürünler de teklif edilebilir.
- 9.2.4. Yüklenici'nin, Ankara'da ofisi bulunmalıdır.
- 9.2.5. Yüklenici, sorumlu personellerinin iletişim bilgilerinde değişiklik olması halinde güncel iletişim bilgilerini en geç 1 hafta içerisinde İdare'ye yazılı olarak bildirecektir.
- 9.2.6. Yüklenici, Bakanlık Bilgi Güvenliği Yönetim Sistemi politika ve prosedürlerine uygun hareket edecektir.
- 9.2.7. Şartnamede geçen tüm ürünler tek bir üretici ailesine ait olacaktır.
- 9.2.8. Kurulumlar tamamlandıktan sonra her 6 (altı) ayda bir sözleşme süresi boyunca health check çalışması yüklenici tarafından yapılacaktır.
- 9.2.9. Yüklenici, teklif edilen SIEM ile ilgili olarak teknik dokümantasyonunu idarenin talep etmesi durumunda Türkçe veya İngilizce olarak sağlayacaktır.
- 9.2.10. Kurulum çalışmaları teklif edilecek ürünler hakkında sertifika sahibi veya ürünler konusunda en az 2 yıl tecrübeli Yüklenici veya üretici personeli tarafından yapılacaktır.
- 9.2.11. Yüklenicinin en az 1 personelinin teklif edilen SIEM ürünü ile alakalı, 1 yıl ya da daha fazla süre boyunca uzmanlık sertifikasına sahip olması gerekmektedir.
- 9.2.12. Yüklenici, kurulum faaliyetleri tamamlandıktan sonra, teklif edilen SIEM ürününe ilişkin olarak Kurum personeline en az **25 (yirmi beş) saat süreli teknik kullanıcı eğitimi** verecektir. Eğitim, kurulum aşamalarını kapsamayacak olup yalnızca sistemin kullanımına, yönetimine ve operasyonel süreçlerine yönelik olacaktır. Eğitim içeriği, kapsamı ve öncelikli konular Kurum tarafından belirlenecek; Yüklenici, bu içerik doğrultusunda gerekli dokümantasyon, uygulamalı senaryolar ve teknik materyalleri sağlayacaktır.

9.3. Log Yönetimi Sistemi ve SIEM (Güvenlik Bilgileri ve Olay Yönetimi) Yetkinlikler ve Gereksinimler

9.3.1. Genel Gereksinimler

- 9.3.1.1. IT altyapısı başta olmak üzere, IoT ve endüstriyel veri kaynaklarının ürettiği standart logları (Syslog, JSON, XML vb.) ve text tabanlı olay kayıtlarını merkezi olarak toplayacak şekilde tasarlanmalıdır.
- 9.3.1.2. Log kaynağında format değişikliği olsa bile kesinti olmadan log toplamaya devam etmelidir. Sistem, bilinen veya standart dışı formatlardaki loglar için arayüz üzerinden esnek ve özelleştirilebilir ayrıştırıcı (Parser) mimarisini desteklemelidir.
- 9.3.1.3. Sistem, merkezi bir platform olarak bütünleşik bir görünürlük sağlamalı ve bütün verileri indeksleyerek gerçek zamanlı analiz yapabilmelidir.
- 9.3.1.4. Sistem; olay kayıtlarını, yapılandırılmış ve yapılandırılmamış veri formatlarını (JSON, Nested JSON, CEF, LEEF, XML, SNMP vb.) standart log kaynaklarından gerçek zamanlı olarak toplayabilmelidir.
- 9.3.1.5. Sistem, beklenmedik anlık log patlamalarında veya lisans limitlerinin zorlandığı durumlarda, merkezi veritabanı ve korelasyon motorunun çökmesini engellemek adına akıllı yük dengeleme mimarisine sahip olmalıdır. Bu durumlarda sistem, merkez sunucuları aşırı yük altında bırakıp performansı düşürmek yerine, veriyi uzak toplama bileşenleri üzerinde yerel disk önbelleğinde (local storage caching/buffer) güvenli bir şekilde sıraya almalıdır. Merkez bileşenlerin (lisans limitleri veya donanım sınırları nedeniyle yeni veri kabul edemediği durumlarda, uzak toplayıcılar üzerinde biriken bu veriler hiçbir şekilde kayba (drop) uğramadan kuyrukta bekletilmeli ve sistem kararlı hale geldiğinde merkeze kayıpsız iletilmelidir.
- 9.3.1.6. Ürün kapasitesi; en az **2500 EPS** ve aynı zamanda en az **100 GB/gün** log işleme kapasitesi sağlayabilmelidir. Ayrıca sistem en az 100 cihaz ve 50 ajan desteklemelidir.
- 9.3.1.7. Teklif edilecek sistem, şartnamede belirtilen lisans GB/Gün veya eps olarak net bir şekilde ürün ve sistem üzerinde görüntülenmeli ve tam uyumlu olarak çalışmalıdır. Üretici veya entegratör firma; "esnek kapasite" veya "yumuşak kısıtlama (soft-lock)" gibi adlar altında, belirtilen lisans sınırları dahilinde olmayan kullanımları barındırmamalıdır. Sistem, taahhüt edilen kapasite sınırları içerisinde hiçbir performans kaybı veya erişim engeli olmaksızın, şeffaf ve kararlı bir şekilde çalışacağını garanti etmelidir.

9.3.2. Log Toplama Yetkinlikleri

- 9.3.2.1. TCP/UDP tabanlı syslog protokolü,
- 9.3.2.2. Dosya tabanlı protokoller (FTP, SCP, SFTP vb.),
- 9.3.2.3. Klasör bazlı log takibi,

9.3.2.4. Veri tabanı tablosundan veri alma,

9.3.2.5. JSON, Nested JSON, CEF, LEEF, XML ve SNMP gibi çoklu endüstriyel format desteği olmalıdır,

9.3.2.6. Ajanlı ve ajansız (syslog vb.) veri toplamayabilmelidir.

9.3.2.7. HMI, OPC Sunucuları ve IoT güvenlik bileşenleri gibi endüstriyel/sensör veri kaynaklarından standart protokoller (Syslog vb.) vasıtasıyla log toplayabilmelidir. Sistem; bu kaynaklardan gelen ham verilerin anlamlandırılabilmesi için özelleştirilebilir ayrıştırıcı (parser) mimarisini desteklemeli, analistlerin bu verilere özel korelasyon kurallarını ve alarm mekanizmalarını sistem arayüzü üzerinden manuel/esnek olarak tasarlamasına imkân tanımalıdır.

9.3.2.8. Mikroservis ve bulut tabanlı veriler dahil olmak üzere; insan tarafından okunabilen metin tabanlı, tek veya çok satırlı (multi-line) olay kayıtlarını, ağ akış verilerini (Netflow, SFlow, IPFix) ve HTTP/S uç noktası (Webhook/API) üzerinden gelen logları esnek bir şekilde sistem içerisine kabul edebilmelidir.

9.3.3. Yüksek Erişilebilirlik ve Performans

9.3.3.1. Sistem; Aktif-Aktif veya Aktif-Pasif mimaride yüksek erişilebilirlik (H.A. / D.R.) çözümlerini desteklemelidir. Sistemin yüksek erişilebilirlik (H.A.) mimarisinde çalışabilmesi için gereken lisanslama modeli, standart log/veri işleme lisanslamasından (EPS veya kapasite) bağımsız ve farklı bir mimari lisans kalemi olarak ele alınmalı ve bu yapıya uygun şekilde teklif edilmelidir.

9.3.3.2. Sistem, merkezi bileşenlere bağlı kalmadan da çalışabilmeli ve bağlantı tekrar sağlandığında uzak noktadaki node kapasitesi dahilinde biriken logları merkeze iletebilmelidir.

9.3.3.3. Sistem; sanallaştırma ve bulut ortamlarında (çalışmaya uygun, dağıtık ve katmanlı bir mimariyi desteklemelidir.

9.3.3.4. Sistem, lisans esnekliği sağlamak ve anlık trafik patlamalarını (burst) tolere etmek adına, dağıtık mimarideki log toplayıcı bileşenleri arasında kullanılmayan anlık EPS kapasitesini gerçek zamanlı ve dinamik olarak yeniden tahsis edebilen ortak bir havuz mekanizmasını desteklemelidir.

9.3.4. Analiz ve Korelasyon Yetkinlikleri

9.3.4.1. Logların aranabilirliği için optimize edilmiş indeksleme yapısına sahip olmalıdır.

9.3.4.2. Olay korelasyonu ve sezgisel analiz yeteneklerine sahip olmalıdır.

9.3.4.3. Kullanıcıların özel dashboard ve raporlar oluşturabilmesini sağlamalıdır.

9.3.4.4. Yapay zeka ve makine öğrenmesi desteği ile anomali tespiti yapabilmelidir.

- 9.3.4.5.** Tarih bazlı analiz, coğrafi konum bazlı korelasyon ve ağlar arası log analizi yapabilmelidir.
- 9.3.4.6.** Otomatik olay algılama ve tehdit avcılığı (threat hunting) için esnek kurallar tanımlanabilmelidir.
- 9.3.4.7.** Risk Based Alerting kapsamını desteklemeli ve çapraz korelasyon yeteneklerini kullanıcı ve varlık bilgilerini kullanarak yapması beklenmektedir.
- 9.3.4.8.** Log kaynağında format değişikliği olsa bile kesinti olmadan log toplamaya devam etmelidir. Sistem, değişen veya yeni eklenen log formatlarının esnek bir şekilde analize ve korelasyona dahil edilebilmesi için arayüz üzerinden kolayca yönetilebilir, özelleştirilebilir ve test edilebilir bir ayrıştırıcı (Parser) mimarisini desteklemelidir.
- 9.3.4.9.** Belirtilen SIEM çözümü, kutudan çıktığı haliyle (out-of-the-box) hazır en az 2500 adet hazır korelasyon kuralı ve rapor şablonu ile birlikte gelmelidir. Güvenlik ve tehdit algılama odaklı kurallar, endüstri standardı olan MITRE ATT&CK framework'ü ile yerleşik olarak eşleştirilmiş (mapping) olmalı ve analist bu eşleştirmeleri doğrudan görebilmelidir.
- 9.3.4.10.** Sistem; yerleşik tehdit istihbaratı (Threat Intel) yönetimine sahip olmalı, harici beslemeleri (feed) otomatik işleyebilmelidir. Ortama bir SOAR çözümü eklenmesi durumunda, SIEM ve SOAR platformları çift yönlü entegrasyon destekleyerek tehdit istihbaratı süreçlerini merkezi olarak koordine edebilmelidir.
- 9.3.4.11.** Sistem; analistlerin operasyonel verimliliğini artırmak, alarmları doğal dille anlamlandırmak veya sorgu süreçlerini hızlandırmak adına üretken yapay zeka (Generative AI / LLM) entegrasyonunu desteklemelidir. Bu yapay zeka asistanı bileşeninin sistem üzerinde aktif olarak kullanılabilmesi için gerekli olabilecek harici büyük dil modeli servislerine (OpenAI, Azure OpenAI vb.) ait API erişim anahtarları (API Key) ve ilgili bulut tüketim maliyetleri Kurum tarafından (Bring Your Own Key - BYOK modeliyle) sağlanacaktır. Sistem, bu harici API anahtarı girildiğinde entegrasyonu yerleşik olarak desteklemelidir.
- 9.3.4.12.** Sistem; IoT ve endüstriyel (OT) süreçlerden toplanan log ve olay verileri üzerinde, Kurumun altyapısına özel güvenlik kurallarının, özelleştirilmiş alarm mekanizmalarının ve panellerin (dashboard) merkezi arayüz üzerinden esnekçe tasarlanmasını desteklemelidir. Sistem, bu endüstriyel kaynaklardan gelen verilerin anlamlandırılması ve görselleştirilmesi için gerekli olan esnek parser (ayrıştırıcı) editörünü yerleşik olarak sunmalıdır.
- 9.3.4.13.** Sistem; entegre çalışacağı dikey OT güvenlik platformlarının oluşturduğu topoloji ve anomali verilerini merkezi arayüzüne alabilmeli, bu verileri güvenlik bakış açısıyla analiz ve alarm ekranlarına sunabilmelidir.

9.3.5. Raporlama ve Uyarı Mekanizmaları

- 9.3.5.1.** Web tabanlı bir arayüz ile tüm raporlar ve alarmlar kolayca yönetilebilmelidir.

9.3.5.2. Sistem, PDF ve CSV formatlarında rapor çıktı almayı desteklemelidir.

9.3.5.3. Kullanıcılara belirli periyotlarda otomatik rapor gönderebilmelidir.

9.3.5.4. ITSM sistemleri ile entegre olabilmeli ve olay bazlı otomatik çağrı açabilmelidir.

9.3.5.5. Sistem; e-posta, webhook, SNMP trap gibi farklı bildirim mekanizmalarını desteklemelidir.

9.3.6. Veri Güvenliği ve Uyumluluk

9.3.6.1. Tüm loglar şifreli iletişim ile taşınmalı ve arşivlenmelidir.

9.3.6.2. Sistem, uluslararası standartlarla uyumlu olmalıdır (ISO 27001, NIST, GDPR vb.).

9.3.6.3. Log bütünlüğünü ve değişmezliğini sağlayan hashing mekanizması bulunmalıdır.

9.3.7. Sistem Kaynak Takibi

9.3.7.1. İşlemci, bellek ve disk kullanımı belirlenen sınırları aştığında otomatik bildirim sağlamalıdır.

9.3.7.2. Sistem kaynak tüketimi geriye dönük olarak izlenebilmelidir.

9.3.7.3. Log ayrıştırma, indeksleme ve arama gibi bileşenler performansı arttıracak şekilde ayarlanabilir ve tasarlanmış olmalıdır.

9.3.8. Entegrasyon ve Esneklik

9.3.8.1. Açık API desteği bulunmalı ve dış sistemlerle entegrasyonu kolay olmalıdır.

9.3.8.2. Basit Otomasyon/Aksiyon özelliklerinin belirtilen sistem üzerinde desteklemelidir.

9.3.8.3. Zafiyet tarama sistemleri, SOAR, SIEM, ITSM ve tehdit istihbarat platformları ile entegre olabilmelidir.

9.3.8.4. STIX/TAXII protokolleri ile açık kaynak tehdit istihbaratı alabilmelidir.

10. GÜVENLİK DUVARI SİSTEMİ YENİLEME VE TEKNİK DESTEK HİZMETİ

10.1. KONU VE KAPSAM

Kurumun bilgi güvenliği altyapısının güçlendirilmesi amacıyla yeni nesil güvenlik duvarı (NGFW) çözümünün temini, kurulumu, entegrasyonu, teknik destek ve eğitimini kapsamaktadır. Proje; ağ trafiğinin denetlenmesi, tehditlerin önlenmesi, kullanıcı ve uygulama bazlı erişim kontrolü ile yüksek erişilebilirlik ve süreklilik esaslarını içermektedir.

10.2. GÜVENLİK DUVARI GENEL HÜKÜMLER

- 10.2.1.** Yüklenici, İdare'nin menfaatleri doğrultusunda çalışmayı ve talimatları doğrultusunda gizlilik esaslarına uygun şekilde hareket etmeyi kabul eder.
- 10.2.2.** Yüklenici Ankara'da bulunmalı ya da Ankara'da yerleşik şubesi bulunmalıdır ve bunu belgelemelidir. Ankara'da şubesi olması halinde bünyesinde İdare'nin bu İş Tanımı kapsamında garantisi altına giren hizmetlere yönelik taleplerine cevap verebilecek sayıda eleman bulundurmaktadır.
- 10.2.3.** Yüklenici, İdare'ye irtibat için telefon numaralarını ve adreslerini sözleşmenin imzalandığı tarihinden itibaren en geç 2 (iki) gün içinde yazılı olarak bildirecektir. Taşınma veya herhangi bir sebeple Yüklenicinin telefon numarasının veya adresinin değişmesi durumunda Yüklenici, İdare'ye yeni adres veya telefon numaralarını en geç 2 (iki) gün içerisinde yazılı olarak bildirecektir.
- 10.2.4.** İstekli, Sanayi ve Teknoloji Bakanlığı tarafından düzenlenen Kamu Bilişim Yetki Belgesine sahip olmalıdır ve teklif dosyasında sunulmalıdır.
- 10.2.5.** İstekli, teklif ettiği tüm donanım ve yazılım ürünlerini satmaya yetkili olduğunu gösterir belgeyi ilgili üreticinin kendisinden veya Türkiye' deki distribütöründen alarak teklif dosyasında sunacaktır.
- 10.2.6.** Yüklenici, şartnamede belirtilen süreler içerisinde hizmetlerin ifası, cihazların aktif çalışır şekilde teslim edilmesi, sözleşme şartlarını sağlamak amacıyla yeterli ve her türden kaynağı sağlamakla yükümlüdür.
- 10.2.7.** Yüklenici, şartnamede belirtilen ürünleri ve hizmetleri İdare'nin teslim öncesinde talep edeceği yerde teslim etmekle ve/veya sağlamakla yükümlüdür.
- 10.2.8.** İşbu şartnamede belirtilen işlerin, şartnamede tarif edildiği şekilde ve anahtar teslimi olarak bitirilmesi esastır. Yüklenici, ihale bedeli dışında hiçbir şekilde ek ücret talep etmeyecektir. Bu sebeple; Yüklenici, işine etki edecek tüm yapısal ve nihai husustan dikkatle gözden geçirmeli ve buna göre tüm aksesuarları temin etmelidir.
- 10.2.9.** Mücbir sebepler dışında oluşabilecek her türlü zarardan Yüklenici sorumludur.
- 10.2.10.** Şartnamedeki herhangi bir maddeyi sağlayamayan teklifler değerlendirme dışı bırakılacaktır.
- 10.2.11.** Teklif edilen tüm Ürünlerin teklifte belirtilecek olan teknik özellikleri, üretici Firmaların kendi web sayfalarında veya teklifle birlikte sağlanacak orijinal teknik dokümanlardaki bilgilerle çelişmeyecektir.
- 10.2.12.** Teklif edilen tüm Ürünler ve şartnamenin ilgili maddelerinde istenilen özellikler ihalenin yapıldığı tarihte ana üreticinin web sayfasından erişilebilen teknik dokümanlarda duyurulmuş, kullanılabilir durumda ve standart üretim olmalı, ihaleye uygunluk açısından değiştirilmiş olmamalıdır.
- 10.2.13.** Yüklenici, teklif ettiği tüm cihazları veya ilgili lisansları, hiç kullanılmamış ve sıfır yeni ürün olarak teslim edilecektir.

- 10.2.14.** Yüklenici, yapılan inceleme ve testler sonucu istenen teknik özellikleri sağlamadığı belirlenen tüm malzeme ve donanımı herhangi bir ücret talep etmeden, istenen özelliklere sahip malzeme ve donanım ile değiştirmekle yükümlüdür.
- 10.2.15.** Yüklenici, teklif ettiği ürün ve hizmetleri İdare'nin belirleyeceği yerde ve ölçütler doğrultusunda kurmakla, hizmet işlemi verecek duruma getirmekle mükelleftir.
- 10.2.16.** Yüklenici, işbu Şartname kapsamındaki yükümlülüklerini yerine getirmek amacıyla gerekli tüm lisans, muvafakat ve yetkileri haiz olduğunu taahhüt eder.
- 10.2.17.** Yüklenici, tüm donanım ve yazılımları "teklif edilen ürün ailesinin sertifikasyonuna sahip" personelleri tarafından kurulacak, konfigüre edilecek ve çalışır halde teslim edecektir.
- 10.2.18.** Yüklenici, kullanacağı tüm cihaz ve parçalar için İdare'nin onayını alarak işe başlayacaktır.
- 10.2.19.** Yüklenici, kurulum faaliyetleri tamamlandıktan sonra, teklif edilen Yeni Nesil Güvenlik Duvarı ürününe ilişkin olarak Kurum personeline en az **25 (yirmi beş) saat süreli teknik kullanıcı eğitimi** verecektir. Eğitim, kurulum aşamalarını kapsamayacak olup yalnızca sistemin kullanımına, yönetimine ve operasyonel süreçlerine yönelik olacaktır. Eğitim içeriği, kapsamı ve öncelikli konular Kurum tarafından belirlenecek; Yüklenici, bu içerik doğrultusunda gerekli dokümantasyon, uygulamalı senaryolar ve teknik materyalleri sağlayacaktır.

10.3. GÜVENLİK DUVARI (2 ADET)

- 10.3.1.** Ürün, aşağıda detayları belirtilen OSI mimarisine uygun çok katmanlı güvenlik modeline sahip olmalıdır.
- 10.3.2.** Güvenlik politikaları özelinde OSI L4 ve L7 katmanları arasında çalışabilmelidir. Bu sayede istenen trafikler L4 (kaynak ip/kullanıcı, hedef ip, hedef port) istenen trafikler L7 uygulama seviyesinde analiz edilebilmelidir.
- 10.3.3.** 7. katmanda uygulama seviyesinde analiz edilmesi gerekmeyen trafik tipleri için (yedekleme trafiği, database senkronizasyonu v.b.) sistemin gereksiz yere performans tüketmesi engellenebilmeli ve sistem verimliliği artırılabilirdir.
- 10.3.4.** Ürün yüksek performans ve düşük gecikme sürelerinin sağlanması amacıyla **ASIC, FPGA veya ICA (Integrated Crypto Assistant)** donanımsal hızlandırma mimarilerinden birine sahip olmalıdır.
- 10.3.5.** Ürün, aktif-aktif ve aktif-pasif yedeklilik senaryolarını desteklemelidir. Herhangi bir donanımsal arıza durumunda yedek cihaz otomatik olarak devreye girmeli, sistem yöneticilerinin manuel bir işlem yapması gerekmemelidir.
- 10.3.6.** Kümeleme yapılan donanımlarda oturumlar donanımın herhangi birisinin arızalanması durumunda desteklenen protokoller için oturum kaybı olmadan otomatik olarak diğer güvenlik duvarı cihazı üzerinde devam edebilmelidir.
- 10.3.7.** Teklif edilecek lisanslar On site spare (OSS), Lab ve benzeri lisanslama modeli olmayacaktır. Aktif ve yedek cihaz aynı ürün modeli olacak ve her ikisinin de ayrı ayrı şartnamede istenilen kendine ait lisansı olacaktır. Aktif cihazda bir sorun olması durumunda tüm trafik kesintisiz, tüm güvenlik kuralları ve lisansları ile yedek cihazdan aynı şekilde devam edecektir. Bu durumda herhangi bir şekilde lisans taşınması (manuel, case açarak vb) yapılan çözümler kabul edilmeyecektir.
- 10.3.8.** Network arayüzlerinin herbiri LAN, WAN, DMZ veya kullanıcı tanımlı bir segment olarak konfigüre edilebilmelidir. İlgili arayüzler 802.1q protokolünü desteklemelidir. Her bir interface için Alias tanımlı girilebilmelidir.
- 10.3.9.** Yerel ağdaki bir ya da birden fazla adres aralığındaki birçok IP'yi istenirse tek bir adres arkasında, istenirse her bir aralığı başka bir tek adres arkasında saklayabilmeli ya da bire bir adres çevrim özelliği (NAT) olmalıdır.

- 10.3.10.** NAT kuralları, Güvenlik kurallarından bağımsız ayrı kural seti olarak tanımlanabilecektir.
- 10.3.11.** Tek bir NAT kuralı ile hem internete çıkış hem de internet geliş yönünde bire bir adres çevrimi için Statik NAT özelliği (NAT) olmalıdır.
- 10.3.12.** Güvenlik Duvarı 802.3 ad LACP desteklemelidir.
- 10.3.13.** Güvenlik Duvarı SNMP v3 desteklemelidir.
- 10.3.14.** Sistem IPv4/v6 Statik ve Dinamik (OSPFv2/v3, BGPv4, RIPv2) Yönlendirme protokollerini desteklemelidir, lisans gerekiyorsa teklife dâhil edilmelidir.
- 10.3.15.** Sistemin SPI (Stateful Packet Inspection) özelliği olmalıdır.
- 10.3.16.** RIP, OSPF, BGP, static ve kaynak tabanlı (policy based) yönlendirme özelliklerine sahip olmalıdır. Multicast routing'i desteklemelidir.
- 10.3.17.** Cihazın Multicast yönlendirme desteği olmalı ve PIM-SM, PIM-SSM, IGMP v2, v3 desteklemelidir.
- 10.3.18.** Site to site ve client to site IPSEC VPN desteği olmalıdır.
- 10.3.19.** Cihaz, IPsec VPN standardını desteklemelidir. IKE şifreleme şemalarını desteklemelidir. 3DES, AES ve AES256 algoritmaları ile paket şifreleme yapabilmelidir. Veri bütünlüğü için MD5, SHA1 ve SHA256 algoritmalarını desteklemelidir. Diffie-Hellman groups 1, 2 ve 5 (Perfect forward secrecy) desteği olmalıdır.
- 10.3.20.** Cihaz GRE tunnel destekleyecektir.
- 10.3.21.** Cihaz IPv6 IPsec destekleyecektir.
- 10.3.22.** NAT64 ve Jumbo frame desteği olmalıdır.
- 10.3.23.** Ağ arayüzü veya zone bazlı kural yazılmasını desteklemelidir.
- 10.3.24.** Microsoft Active Directory ile entegre olarak kişi ve grup bazında kural yazılabilecektir. Kullanıcıya göre kural yazma sadece kimlik bilgisi gönderen uygulamalarla sınırlı olmayacaktır. Log kayıtlarda kullanıcı ismi de yer alacaktır.
- 10.3.25.** Kullanıcı entegrasyonu için yönetici (administrator) hesabına ve Microsoft Active Directory yapısında herhangi bir değişikliğe ihtiyaç olmayacaktır.
- 10.3.26.** Kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS, LDAP ve Microsoft Active Directory üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.
- 10.3.27.** Teklif edilen sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama, Ping6, IPv6 captive portal, IPv6 FQDN adresleri desteklenmelidir.
- 10.3.28.** İşletim sistemi ve yazılım güncellemelerini web ara yüzü, TFTP üzerinden yapılabilmelidir.
- 10.3.29.** Cihazın detayları aşağıda belirtilen bant genişliği yönetim özelliği olmalıdır.
- 10.3.30.** Kaynak ip/ağ, kullanıcı/kullanıcı grubu, hedef ip/ağ ve servis bazında bant genişliği politikası yazılabilmelidir.
- 10.3.31.** Spesifik uygulama (örneğin Youtube) ve uygulama kategorisi (örneğin Update) bazında bant genişliği politikası yazılabilmelidir.
- 10.3.32.** Zaman aralığı bazında bant genişliği politikası yazılabilmelidir (örneğin mesai saatleri içerisinde gibi.).
- 10.3.33.** Önerilecek güvenlik duvarı üreticisi, güncel "Gartner Magic Quadrant Enterprise Network Firewalls" raporunda "Leaders" kategorisinde yer almalıdır.
- 10.3.34.** Teklif edilecek tüm ürünler üreticinin global destek merkezi tarafından 7x24 destek hizmeti dahil şekilde tekliflendirilecektir. Kurum, üreticinin global destek merkezine 7x24 case açabilecektir. Acil durumlar için telefonla üreticinin global destek merkezinden eş zamanlı destek alınabilmelidir. Bu özellikler için ilave lisans gerekmesi durumunda teklife dahil edilmelidir.
- 10.3.35.** Cihazlar mimari açıdan stateful inspection, IP Paket Filtreleme ve Uygulama Tanıma özelliklerini bünyesinde bulundurmalı ve aşağıdaki güvenlik servislerine sahip olmalıdır.

- Firewall
 - IPSEC VPN,
 - Uygulama kontrolü (Application Control)
 - SSL Deep Inspection
 - Atak Engelleme (IPS)
 - Anti-Virus/AntiMalware
 - Web (URL) Filtreleme
 - DNS Security/DNS Filtreleme
- 10.3.36.** Güvenlik kuralları özelinde L7 güvenlik servisleri aktif edilebilmelidir. Bu kapsamda aşağıda listelenen güvenlik servisleri tercihe bağlı olarak seçilebilmelidir.
- Uygulama kontrolü (Application Control)
 - SSL Deep Inspection
 - Atak Engelleme (IPS)
 - AntiVirus/AntiMalware
 - Web (URL) Filtreleme
 - DNS Security/DNS Filtreleme
- 10.3.37.** Teklif edilecek güvenlik duvarı ürünleri üzerinde aşağıda detayları belirtilen sanal güvenlik duvarı özelliği (virtual firewall/virtual domain) olmalıdır ve her bir cihaz üzerinde en az 10 adet sanal güvenlik duvarı lisansı olacak şekilde lisanslanmalıdır.
- 10.3.38.** Sistem üzerinde detayları aşağıda belirtilen uygulama kontrol özelliği bulunmalıdır.
- 10.3.39.** Sistemin uygulama kütüphanesinde en az 2000 (iki bin) adet uygulama yer almalıdır.
- 10.3.40.** Uygulama kütüphanesinde yer alan tüm uygulamalar aşağıda belirtilen parametrelere göre kategorize edilmiş olmalıdır.
- Uygulama davranışına göre (uzak erişim, video/ses, sosyal medya, bulut uygulaması, v.b.)
 - Risk seviyesine göre (Critical, High, Medium, Low v.b.)
 - Erişim yöntemine göre (Client-server, browser tabanlı, P2P gibi)
- 10.3.41.** Uygulama kontrol özelliği Microsoft Active Directory ile entegre çalışabilecek bu sayede Microsoft Active Directory’de tanımlı olan kullanıcı ve kullanıcı grupları bazında uygulama kontrol kuralları tanımlanabilecektir.
- 10.3.42.** Kuruma özel uygulamaların sisteme tanıtılması özel imza oluşturmak suretiyle mümkün olmalıdır.
- 10.3.43.** Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir.
- 10.3.44.** Sistemin güncel saldırıların engellenmesi amacıyla aşağıda detayları belirtilen atak engelleme (IPS) özelliği olmalıdır.
- 10.3.45.** IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak da yapılabilirdir.
- 10.3.46.** Her bir IPS imzası için aşağıdaki aksiyonlar alınabilmelidir.
- İzin ver (pass)
 - İzin ver ve olay kaydı al
 - Paketi düşür (block)
 - Paketi düşür ve session’ı sonlandır (Reset/Reject)
- 10.3.47.** Veritabanında yer alan imzalar aşağıdaki tanımlara göre filtrelenebilmelidir.
- Kullanılan uygulamaya göre (IIS, Oracle, SQL, Apache gibi)
 - İşletim sistemine göre (Windows, Linux, Solaris gibi)
 - Protokole göre (HTTP, HTTPS, FTP, DNS gibi)
 - CVE koduna göre
 - Risk seviyesine göre (Kritik, Yüksek Risk, Orta Risk, Düşük Risk gibi)

- Hedef işletim sistemine göre (client ve/veya server)
- 10.3.48.** Rate tabanlı saldırı tanımları içerisinde ne kadar sürede kaç adet istekte bulunulabileceği tanımlanabilmelidir.
- 10.3.49.** IPS sistemi Botnet aktivitelerini tespit edebilmeli ve engelleyebilmelidir.
- 10.3.50.** Cihaz üzerindeki IPS imzaları CVE id lerine, kritiklik seviyelerine ve host (client/server) tipine göre aranabilmektedir.
- 10.3.51.** IPS sisteminin saldırıları karşılama biçimi, sistem yöneticisi tarafından her bir imza için ayrı ayrı ayarlanabilmelidir.
- 10.3.52.** IPS özelliğinde saldırılara karşı kullanılan filtreler internet üzerinden güncellenebilmelidir. Ayrıca eğer istenirse, imza güncellemeleri kullanıcı müdahalesi olmadan otomatik olarak da yapılabilir.
- 10.3.53.** Cihazın detayları aşağıda belirtilen DNS Security/DNS Filtreleme özelliği olmalıdır. Bu özellikler için ek lisans varsa eklenmelidir.
- 10.3.54.** Botnet C&C ve Phishing domain adreslerine yapılan lookup sorguları engellenebilmelidir.
- 10.3.55.** Yeni register edilmiş (Newly Registered Domains) domain'ler için DNS sorgularının engellenmesi sağlanmalıdır.
- 10.3.56.** İstenmeyen domain adreslerine yapılan erişimlerin engellenmesi veya ilgili domain'e ait gerçek ip adresi yerine belirlenen farklı bir ip adresinin cevap olarak dönmesi sağlanabilmelidir.
- 10.3.57.** DNS sorguları limitlenerek DNS Flood koruması sağlanabilmelidir.
- 10.3.58.** DNS over HTTPS (DoH) ve DNS over TLS (DoT) trafikleri analiz edilebilmelidir.
- 10.3.59.** DNS Safe Search özelliği desteklenmelidir.
- 10.3.60.** DNS Translation yapabilmelidir.
- 10.3.61.** Aşağıdaki DNS saldırı tipleri engellenebilmelidir.
- DNS Tunnelling
 - DNS Exfiltration
 - DNSCat2
 - C2 Server Identification
 - Low Bandwidth DNS Tunnel Upload
 - DGAs
- 10.3.62.** DNS güvenliği mimarisi Yapay Zekâ (AI) temelli global veritabanını gerçek zamanlı (real time) olarak kullanabilmeli, bu özellik desteklenmiyor ise lokalde yapay zekâ mimarisini kullanarak analiz yapabilmelidir.
- 10.3.63.** Cihazın detayları aşağıda listelenen "SSL Deep Inspection" özelliği olmalıdır.
- 10.3.64.** İstenen web adresleri ve domain'ler için SSL Inspection istisnası uygulanabilmelidir. Wildcard FQDN istisna objeleri desteklenmelidir.
- 10.3.65.** SSL anomaly'lerini ve yazılan istisnai SSL erişimlerini loglayabilmelidir.
- 10.3.66.** Süresi geçmiş (expired) sertifika kullanan sunucu erişimlerini bloklayabilmelidir.
- 10.3.67.** Doğrulama süresi geçmiş (validation timeout) ya da doğrulanamayan (validation failed) sertifika kullanan sunucu erişimlerini bloklayabilmelidir.
- 10.3.68.** Sistem üzerinde detayları aşağıda iletilen URL Filtreleme özelliği bulunmalıdır.
- 10.3.69.** Üreticinin global kategori veritabanında yer alan tüm URL adresleri ve kategori bilgileri sözleşme süresi boyunca otomatik olarak güncellenecek ve teklif edilecek sistemin bu veritabanından eş zamanlı faydalanması mümkün olacaktır.
- 10.3.70.** Karaliste ve beyazliste özelliği olmalıdır. Bu sayede direk url adresi, regex ve wildcard formatında tanımlı adreslere erişime izin verebilmeli veya engelleme yapabilmelidir.
- 10.3.71.** USOM gibi harici karaliste kaynakları engellenebilmeli ve otomatik olarak güncellenebilmelidir.
- 10.3.72.** Çoklu harici karalisteleri desteklemelidir.

- 10.3.73.** URL bloklama ekranı özelleştirilebilmelidir.
- 10.3.74.** URL filtreleme özelliği Microsoft Active Directory ile entegre çalışabilecek bu sayede Microsoft Active Directory’de tanımlı olan kullanıcı ve kullanıcı grupları bazında URL filtreleme kuralları tanımlanabilecektir.
- 10.3.75.** URL Filtreleme özelliğinde kategori ve/veya URL adresleri ve/veya kullanıcı sayısı bazında bir lisanslama veya limitasyon olmamalıdır. Eğer farklı lisans seçenekleri var ise kullanıcı ve/veya kategori bazında limitsiz lisanslama ile teklif edilmelidir.
- 10.3.76.** Sistemin detayları aşağıda belirtilen Antivirüs özelliği olacaktır;
- 10.3.77.** Sistem aşağıda belirtilen protokoller aracılığıyla yapılan malware trafiklerini tespit edip engelleyebilmelidir.
- HTTP(S)
 - POP3(S)
 - FTP
 - CIFS/SMB
- 10.3.78.** Farklı kullanıcı veya kullanıcı grupları için farklı anti-virüs politikaları oluşturulabilmelidir.
- 10.3.79.** Bilinen virüsler için imza temelli bloklama yapabilmelidir.
- 10.3.80.** Akan dosya trafiğini tarayabilmelidir.
- 10.3.81.** Sistem, yukarıda belirtilen protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir.
- 10.3.82.** Antivirüs sistemi internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmeli, gerekmesi durumunda antivirüs veritabanı manuel olarak güncellenebilmelidir.
- 10.3.83.** Antivirüs sistemi, akıllı telefonlara yönelik mobil malware’leri tespit edebilme ve engelleme özelliğine sahip olmalıdır. Bu özellik için ek lisans gerekiyorsa teklife eklenmelidir.
- 10.3.84.** AntiVirus sistemi Yapay Zeka (AI) destekli çalışabilmelidir. Bu özellik için ek lisans gerekiyorsa teklife eklenmelidir.
- 10.3.85.** Makine öğrenme (ML) ve tespit modellemesi otomatik olarak global veritabanı üzerinden güncellenebilmelidir.
- 10.3.86.** Yapay zeka (AI) tarafında tespit edilmiş olan zararlı yazılımlar AntiVirus loglarında ayrı bir şekilde gösterilebilmelidir.
- 10.3.87.** Sistem, henüz lokal veritabanında yer almayan virüslere karşı anlık, gerçek zamanlı istihbarat servis sorgulaması (real-time query) yapabilmelidir. Bunu yaparken dosyanın kendisi paylaşımlı bulut servisine gönderilmemelidir. Bu özellik için ek lisans gerekiyorsa teklife eklenmelidir.
- 10.3.88.** Çok yeni tespit edilen ancak cihaz üzerindeki lokal AntiVirus veritabanında henüz yer almayan virüslere karşı gerçek zamanlı koruma sağlayabilmelidir. Bunu yaparken dosyanın kendisi paylaşımlı bulut servisine gönderilmemelidir.
- 10.3.89.** Üreticinin Sandbox sensörleri ve Sandbox teknolojisini kullanan diğer kurumların Sandbox ürünleri tarafından tespit edilmiş zararlı veritabanından eş zamanlı faydalanması mümkün olmalıdır. Bu özelliğin kullanımı için dosyanın kendisinin buluta gönderimi gerekmemelidir.
- 10.3.90.** Ürün, saniyede en az 500.000 (beşyüzbin) yeni oturum açabilme (cps) kapasitesine sahip olmalıdır.
- 10.3.91.** Ürün, eş zamanlı olarak en az 25 (yirmibeş) milyon oturumu (session) desteklemelidir.
- 10.3.92.** Ürün, en az 50 (elli) Gbps L7 firewall (uygulama kontrol) performans değerine sahip olmalıdır.
- 10.3.93.** Ürün en az 10 (on) Gbps Threat Protection (Tehdit Engelleme) performans değerine sahip olmalıdır.
- 10.3.94.** Ürün, en az 50 (elli) Gbps IPSEC VPN performans değerine sahip olmalıdır.

- 10.3.95.** Ürün, SSL Deep Inspection ve IPS servisi aktif edildiğinde en az 9700 (dokuzbinyediyüz) yeni bağlantı isteğini (SSL cps) desteklemelidir. Bu değerin herkese açık datasheet'lerde yayınlanmadığı durumda üretici bu değeri sağladığını yazılı olarak taahhüt edecektir.
- 10.3.96.** Ürün, SSL Deep Inspection ve IPS servisi aktif edildiğinde en az 3.000.000 (üçmilyon) oturumu (SSL concurrent session) desteklemelidir. Bu değerin herkese açık datasheet'lerde yayınlanmadığı durumda üretici bu değeri sağladığını yazılı olarak taahhüt edecektir.
- 10.3.97.** Ürün, SSL Deep Inspection ve IPS servisi aktif edildiğinde en az 10 (on) Gbps performans (SSL inspection throughput) değerine sahip olmalıdır. Bu değerin herkese açık datasheet'lerde yayınlanmadığı durumda üretici bu değeri sağladığını yazılı olarak taahhüt edecektir.
- 10.3.98.** Ürün, aynı anda en az 4 adet SFP28/SFP+, 4 adet SFP/SFP+, 16 adet SFP ve 8 adet GE/5GE RJ45 bağlantı desteğine sahip olmalıdır.
- 10.3.99.** Cihaz üzerindeki güç kaynakları yedekli olacak şekilde teklif edilmelidir.

10.4. GÜVENLİK DUVARI LOGLAMA SİSTEMİ (1 ADET)

- 10.4.1.** Teklif edilecek sistem bu şartname içerisinde teklif edilecek olan firewall ürünlerine ait logların kayıt altına alınması, izlenmesi ve detaylı raporlanmasını sağlamalıdır.
- 10.4.2.** Teklif edilen ürün sanal appliance olarak teklif edilecektir ve VMware veya HyperV platformu üzerinde çalışmayı desteklemelidir.
- 10.4.3.** Herhangi bir anda kurulmuş olan bağlantıları gerçek zamanlı olarak izleyebilme olanağı olacaktır.
- 10.4.4.** Cihaz üzerinden geçen tüm trafiğin günlüklerde tutulması, istenen kısıtlara göre (En az IP, IP aralığı, ağ, protokol, zaman) filtrelenebilmesi ve aktif bağlantıların gerçek zamanlı izlenebilmesi sağlanacaktır.
- 10.4.5.** Gün, saat veya haftalık periyotlarda yapılandırılabilen otomatik kayıt arşivleme özelliği olacaktır.
- 10.4.6.** Güvenlik duvarları ile kayıt sunucusu arasında iletişimin sağlanamaması durumunda oluşturulan kayıtlar, bağlantı sağlanana kadar güvenlik duvarının kendi üzerinde tutulabilmelidir.
- 10.4.7.** Yönetilen ağ güvenlik duvarlarına ait performans ve güvenlik duvarları üzerinden geçen trafik ile ilgili bilgileri geçmişe yönelik olarak gösterebilme özelliği desteklenecektir.
- 10.4.8.** Merkezi yönetim dâhilinde bulunan bileşenlere ait anlık ortalama CPU, boş disk alanı, firewall, firewall cluster üzerinden akan tüm uygulamalar, kullanıcı IP adresleri ve dâhili kullanıcı isimleri gibi değerler anlık ve sürekli olarak görüntülenebilecektir.
- 10.4.9.** Önerilen kayıt yönetim sistemi geçmişe yönelik olarak raporlama yapabilme özelliğine sahip olacaktır. Örneğin bant genişliği kullanımı, uygulama denetimi, URL filtreleme ile ilgili istenen tarih aralıklarında raporlar üretebilecektir.
- 10.4.10.** Tutulan kayıt alanları baz alınarak özelleştirilmiş sorgular yazılabilmeli ve bu sorguların çıktıları, tablo, pie-chart şeklinde raporlar içerisine konulabilmelidir.
- 10.4.11.** Pdf formatında rapor üretebilmeli ve üretilen raporları belirtilen e-mail adreslerine otomatik veya elle gönderebilmeli, ftp veya web sitelerine otomatik olarak yükleyebilmelidir.
- 10.4.12.** Kayıtları ftp veya benzer bir protokolle harici bir Sunucu veya Depolama alanı üzerinde yedekleme yapıp arşivleyerek kayıtların yedekliliği sağlayabilmelidir.
- 10.4.13.** Teklif edilen sistemlerin en az 3 yıl yazılım/donanım garantisi bulunmalıdır. 3 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.
- 10.4.14.** Operasyonel hız kazanımı için AI Assistant özelliği çözümde bulunmalı ve lisanslı olarak verilmelidir.

10.4.15. AI Assistant ile analistin olay çözüm süresini desteklemek üzere aşağıdaki yetenekler sağlamalıdır.

10.4.15.1. Event Monitor üzerinde filtreleme, gruplama ve özetleme yapabilmelidir.

10.4.15.2. Tanımlanan senaryolara göre Event Handler kuralı önerebilmelidir.

10.4.15.3. IOC niteliğindeki file hash değerleri ile log/incident ilişkisi kurma ve araştırma yapabilmelidir.

10.4.15.4. Analiz sonucuna göre ilgili özet ekranlar gösterebilmelidir.

10.5. GÜVENLİK DUVARI İŞİN SÜRESİ VE HİZMET DETAYLARI

10.5.1. Yüklenici, teknik şartnamede tanımlanan tüm işleri ve hizmetleri 60 (Altmış) takvim günü içerisinde tamamlayacaktır. (Cihaz kurulumu ve çalışır halde teslimini kapsayacaktır.) Yüklenici iş planı hazırlayacak, Bilgi Teknolojileri Daire Başkanlığı onayına istinaden iş planına uygun olarak kurulumlar yapılacaktır.

10.5.2. Temin edilecek tüm ürünler, lisanslar “Kurum Adına” kaydedilecek ve lisanslanacaktır.

10.5.3. Arıza bildirim zamanı, İdare’nin Yükleniciye veya temsilcisine yazılı veya mail bildirimde bulunduğu zamandır. Cihazların arızalarının çözülmesi, İdare ve Yüklenici arasında e-posta veya yazılı olarak arızaların giderildiğinin kayıt altına alınması ile tamamlanmış kabul edilecektir.

10.5.4. Hizmet süresince ortaya çıkabilecek tüm bakım ve onarım Yüklenici tarafından, belirtilen hizmet seviyeleri süreleri içerisinde yerine getirilecektir. Yüklenici, hizmet süresinde İdare tarafından hizmet kapsamında olmak üzere talep edilen hiçbir mal ve hizmet için her ne koşulda olursa olsun İdare’den ayrıca ücret talep etmeyecektir.

10.5.5. Hizmet süresi içinde doğabilecek her türlü arıza ve hasarlardan (kullanım hataları hariç) Yüklenici sorumlu olacaktır.

10.5.6. Arızanın çözüm süresi Yüklenicinin İdare’ye yazılı veya e-posta ile işin tamamlandığını bildirmesi veya İdare’ye isim-imza karşılığı teslim edeceği servis formunda belirtilen saat ile tespit edilir.

10.6. GÜVENLİK DUVARI ARIZA ÇÖZÜM/MÜDAHALE VE CEZAI KOŞULLAR

10.6.1. Yüklenici sözleşme süresince çağrı açılacak tüm iletişim bilgilerini (Firma, İlgili Kişi, Telefon, e-Mail vb.) İdare’ye kabul dokümanlarında teslim edecektir.

10.6.2. İdare/Kurum tarafından bildirilen arızalar yüklenici tarafından kayıt altına alınmalı, istenildiğinde raporlanabilmelidir.

10.6.3. Yüklenici hizmet süresince yukarıda tanımlanan hizmetleri İdare’ye sağlayacak ve aşağıdaki tablolarda belirtilen müdahale ve çözüm sürelerine riayet edecektir.

Tablo A: Güvenlik Duvarı Müdahale ve Çözüm Süreleri

GRUP	HİZMET PENCERESİ	MÜDAHALE SÜRESİ	ÇÖZÜM SÜRESİ
A	7x24	Azami 2 saat	Azami 8 saat
B	7x24	Azami 4 saat	Azami 48 saat
C	7x24	Azami 48 saat	Azami 240 saat
D	5x8	İdare ve Yüklenici tarafından ortaklaşa belirlenir	

Tablo B: Güvenlik Duvarı Arıza ve Kesinti Grup Tanımları

GRUP	TANIM
A	Ciddi Kesintiler Örnek: Sözkonusu sistemin tamamen işlemez duruma gelmesi ya da bir uygulamanın tamamen durması. Söz konusu sistemin önemli bir fonksiyonunun doğru çalışmaması. Sistemin bazı fonksiyonlarının doğru çalışmaması ya da gereğinden fazla yavaşlaması.
B	Majör İş Kesintileri - Kısmi Hizmet Kaybı Örnek: Tepki süresi ve yavaşlık problemleri Sistem yönetim konsolundan sisteme ulaşamaması Sistemin çalışmasını etkileyen fakat sistemi durdurma noktasına getirmeyen arızalar.
C	Minör İş Kesintileri - Bir grup kullanıcının etkilendiği durumlar Örnek: Sistemin çalışmasını etkilemeyen veya bakım sırasında ortaya çıkmış düzenleyici ve arıza önleyici tedbirler.
D	İdare Tarafından Talep Edilen Teknik Destek

10.7. GÜVENLİK DUVARI GİZLİLİK VE SORUMLULUK

10.7.1. Hizmetin ifası sebebiyle bu işe ait ve işin yürütülmesi esnasında İdareye tanzim olunan her türlü belge, rapor, istatistik verisi, bilgisayar kayıtları ve sair materyalin, yazılım kodlarının ve verinin mülkiyeti ve bunlar üzerindeki yayma, çoğaltma, işleme ve umuma iletim şeklindeki her türlü fikri mülkiyet hakkı İdare'ye aittir. Yüklenici, bu bilgileri, istemesi halinde İdare'ye teslim edecek ve kendi kopyasını bir daha ulaşılamayacak şekilde imha edecektir. 3. Şahıslar/Firmalar ile paylaşamayacaktır.

10.7.2. Bu gizlilik yükümlülükleri, bu Yüklenici ile yapılacak sözleşmenin sona ermesi veya feshinden sonra da devam edecek ve geçerli olacaktır.

10.7.3. Yüklenici, tüm İş Sağlığı ve Güvenliği koşullarında çalışmayı ve İSG'den doğacak tüm sorumluluğun kendisine ait olduğunu kabul eder.

12. VERİ DEPOLAMA ÜNİTESİ

12.1. İDARE'nin 2 adet Storage IBM V7000 ve IBM V7200 modelleri mevcut olup ürünlerin lisans, güncelleme ve parçalı bakım desteğinin sağlanması hizmeti alınacaktır.

12.2. Mevcut IBM FlashSystem 7200 ve IBM Storwize V7000 ürünlerinin üretici garantisi 1 (bir) yıllık olarak 'Proactive Support for Storage' seviyesinde teklife eklenmelidir.

12.3. Yüklenici, bakım ve detek hizmetini çözemediği bir sorun olduğunda, üretici veya Türkiye dağıtıcısından destek alacaktır.

13. GENEL ŞARTLAR

13.1. Yukarıda tarifleri yapılan tüm ürünlerin, teknik destek noktasında Yüklenici firmanın yetersiz kaldığı noktalarda teknik desteği, üretici firma veya bu ürünlerin Türkiye

distribütörleri ve/veya yetkili servisleri verecektir. Bu durum İDARE'nin istemesi durumunda teyit edilecektir.

- 13.2.** 6. Maddede sayılan donanımlar ve yazılımlar Türkiye Şeker Fabrikaları A.Ş. Genel Müdürlüğü ile yukarıda ismi yazılı Fabrikalarda bulunmaktadır. Söz konusu donanımlara bulundukları yerde parçalı bakım yapılacaktır.
- 13.3.** Sözleşme süresi içinde 6. maddedeki tabloda bulunan ancak daha sonra herhangi bir sebeple kullanımdan kaldırılan bir ürün bakım kapsamından çıkarılabilecektir. Bu durumu Yüklenici aynen kabul etmiş sayılacaktır.
- 13.4.** Yüklenici stoklarında yeterli miktarda yedek parça bulunduracaktır.
- 13.5.** Bir donanımın tamiri mümkün olmayan parça değişikliklerinde orijinal parçanın aynı özelliklerinde ya da daha üstün özellikte yeni parça takılacaktır. Bir donanımın tümünün değişmesi gerekirse, değişecek donanım İDARE'nin kullandığı mevcut ürünlerden biri veya İDARE'nin onayladığı diğer bir ürün olacaktır.
- 13.6.** Teklifler Türk Lirası olarak ekte yer alan tablodaki gibi donanım grubuna ait birimler üzerinden yıllık olarak verilecek, donanım sayıları ile birim fiyatlar çarpılarak toplam yıllık ücret hesaplanacaktır.
- 13.7.** Ödemeler 4. Madde de KAPSAM başlığı altında açıklandığı şekilde yapılacaktır.
- 13.8.** İDARE'nin Parçalı Bakım kapsamındaki arızasını Yükleniciye bildirdiği günden başlamak üzere Arıza Giderme Süresi başlamış olacaktır. Arıza Giderme Süresi içerisinde giderilemeyen arızalar söz konusu arızalı donanıma isabet eden aylık bakım ücretinin %2'si oranında bulunacak olan ücretlerin geçen her 1 (bir) gün için hesaplanan miktarları yapılacak dönem ödemelerinden kesilir. Arıza Giderme Süresini aşan saatler güne tamamlanacak ve kesintiler (Cumartesi, Pazar günleri de dahil) günlük olarak yapılacaktır.
- 13.9.** İDARE, Yükleniciye bilgi vermek suretiyle donanımların yerini değiştirmek isteyebilir. Yüklenicinin buna itiraz etme hakkı olmadığı gibi bakım ücretlerinde artırma teklifinde de bulunamaz. Yeri değiştirilecek donanımın sökülmesi, paketlenmesi, nakliyesi ve yeni yerde kurulması Yükleniciye ait olacaktır. Bakım süresi içerisinde İDARE'nin alacağı herhangi bir yeni ürünün kurulumu ve üzerinde çalışan işletim sistemlerinin bakımı da Yükleniciye ait olacaktır.
- 13.10.** Bir donanımdaki arızanın sık tekrarlanması durumunda, donanımın tamamı İDARE'nin yazılı talebi üzerine, İDARE'nin kullandığı mevcut marka ve modellerden biri veya üst modeli olmak üzere yeni bir ürünle değiştirilir. Arızanın sıklığı; bir cihaz üzerinde aynı sebepten 1 (bir) ayda 3 (üç) kereden fazla olursa İDARE donanımın değiştirilmesini talep edebilecektir.
- 13.11.** Yüklenici 7 gün x 24 saat ulaşılabilecek destek teknik personellerine sahip olacak ve bu personellerin bilgisini İdare ile paylaşacaktır. İdare tarafından açılan açılan arıza ve

çağrı kayıtlarını İDARE'nin istemesi halinde Gün-Ay-Yıl, Saat olarak İDARE'ye rapor edecektir.

- 13.12.** Mevcut sarf malzemelerini kullanan cihazların değiştirilmesi sonucu takılan yeni cihazların da mevcut sarf malzemelerini kullanabilmesi tercih nedenidir.
- 13.13.** Arıza bildirimi İDARE'nin Ankara'da bulunan Genel Müdürlük Bilgi Teknolojileri Dairesi veya direk arızanın meydana geldiği Fabrika tarafından yapılır. Yüklenici İDARE'ye, bir merkeze ait telefon numaraları verecektir. Arıza, Yükleniciye bildirildiği andan itibaren başlamış olacaktır. Ayrıca arıza; faks, telefon veya e-mail yoluyla Yükleniciye bildirilebilir. Bu konuda İDARE'deki kayıtlar esas alınacaktır.
- 13.14.** Yüklenicinin gönderdiği elamanlar Genel Müdürlük ve Taşra Teşkilatının çalışma şartlarına uygun davranmak zorundadır. Çalışma sırasında Genel Müdürlüğün veya Taşra Teşkilatının görevli personeli Yüklenicinin çalışmasına nezaret edecektir.
- 13.15.** Genel Müdürlüğün veya Taşra Teşkilatının personeli bulunmaksızın Yüklenici, sistemlere müdahale edemez.
- 13.16.** Deprem, yangın, afet, su baskını gibi mücbir sebeplerden meydana gelecek arızalardan Yüklenici sorumlu olmayacaktır. Ancak, bu hallerde değiştirilecek parça bedelleri İDARE tarafından karşılanacak, işçilik ve onarım için Yüklenici ayrıca ücret talebinde bulunmayacaktır.
- 13.17.** İDARE'ye bağlı Şeker, Makine, EMAF Fabrikaları, Şeker Enstitüsü ve Afyon, Erzincan, Turhal Makine İmalat Birimlerinde meydana gelecek Network arızalarının giderilmesi de Yüklenici firmaya ait olacaktır.
- 13.18.** Network Ürünleri Parçalı Bakım TABLO 1.1 ve TABLO 1.2 ürünleri ihalesini alan Yüklenici, sözleşmenin imzalanmasından itibaren Network ürünleri, Windows Server İşletim Sistemleri, Active Directory, Exchange ve sunucu sanallaştırmaları konularında deneyimli en az 1 (bir) elemanını 1 (bir) hafta içerisinde Genel Müdürlüğümüzde kurulu Bilgi Teknolojileri Daire Başkanlığı'nda görevlendirecek ve var olan sistemler gözden geçirilecek, var ise önleyici tedbirler (program güncellemesi, yedekleme mekanizmaları, yeni yazılımların yüklenmesi, güvenlik ayarlarının tanımlarının kontrolü, Fabrika ve Genel Müdürlükte bulunan sunucular arasındaki replikasyon işlemleri vb.) karşılıklı mutabık kalınarak Yüklenici elemanlarınca alınacaktır. İDARE'ye tahsis edilen personelin, İDARE tarafından yetersiz görülmesi durumunda değiştirilmesi talep edilebilecektir. Sözleşme imzalanmasını müteakip Genel Müdürlüğümüzde yapılacak olan çalışmalarda Network ve Internet trafiğini aksatabilecek işlemler için İDARE, yüklenici elemanlarından mesai saatleri dışında yapmasını talep edebilecektir.
- 13.19.** 1. Kısım ihalesini alan Yüklenici, tüm Şirket lokasyonlarında (Genel Müdürlük ve Fabrikalarda) oluşacak network sorunları, internet problemleri, fabrikalar arası haberleşme sorunları vb. konularda sorunu belirleyecek ve ilgili arızayı tespit ederek arızayı giderecek,

sorun farklı firmayı ilgilendiren ürünle ilgili ise gerekli bilgilendirmeyi ve yönlendirmeyi Şirkete yapacaktır.

13.20. 1.Kısım ihalesini alan Yüklenici, Şirketin merkez teşkilatında kurulu (Genel Müdürlük) Sistem Odasında kabinlerde mevcut gereksiz cihazları kabinden çıkartarak veya farklı kabine takarak düzenleme yapacak, boşa çıkan kabinleri sistem odasından çıkartacak, kabinlerin elektrik ve data kablolarında düzenleme ve etiketleme yapacaktır.

13.21. Genel Müdürlüğümüzde operasyonel işleri yapacak personelde asgari aşağıdaki özelliklerin bulunması gerekmektedir.

13.21.1. 4 yıllık Fakülte mezunu ve en az 3 yıllık mesleki tecrübeye sahip olmalı,

13.21.2. Microsoft Server ürün ailesine yüksek hakimiyeti olmalı,

13.21.3. Windows sistem kurulumu, yönetimi, güvenlik, performans analizi, problem yönetimi, yama ve güncellemelerin yüklenmesi, yedekleme ve kabuk programlama konularında tecrübeli olmalı,

13.21.4. IIS, Exchange, Active Directory ve domain kurulumları konusunda bilgi sahibi olmalı,

13.21.5. Yedekleme ve disk sistemlerinde (Storage) deneyimli olmalı,

13.21.6. SAN (Storage Area Network) ve WAN/LAN konusunda bilgi sahibi olmalıdır.

13.21.7. Yüklenici Operasyonel işlerle ilgili mevcut personelin çözemediği sorunları daha yetkin personel/personeller görevlendirerek çözecektir.

13.22. Yüklenici bu şartname kapsamında gizlilik arz eden şifreler, IP'ler, kullanıcı vb. bilgileri üçüncü şahıslara vermeyecek ve onlarla paylaşmayacaktır.

13.23. Yüklenici vereceği hizmetler ile ilgili ileride bir ihtilafa düşmemesi için teklif hazırlama aşamasında İDARE'nin Bilgi Teknolojileri Daire Başkanlığı ile görüşerek Ankara Merkezdeki donanım alt yapısını görüp ihtiyaç duyduğu ve tereddüt ettiği tüm konular hakkında bilgi alabilecektir.

13.24. İhale kapsamındaki tüm ürünler için ilgili Yüklenici, Merkez ve Fabrikalarımızda oluşacak ürünle ilişkili tüm sorunlardan sorumlu olacak ve Arıza Giderme Süreleri içerisinde arızaları giderecektir.

14. ARIZA MÜDAHALE / ÇÖZÜM SÜRELERİ ve SERVİS ZAMANLARI

Arıza Giderme Süresi; İDARE tarafından Yükleniciye bildirilen bir arızanın giderilme süresi olup bu süre Genel Müdürlük Merkez Teşkilatı ve Ankara Etimesgut kampüsündeki fabrikalar için 2 (iki), Taşra Teşkilatı için 3 (üç) iş günüdür.

Önem Seviyesi	Açıklama	Müdahale	Servis Zamanı
Acil	Servis Kesintisi	2 saat	7 gün x 24 saat
Acil	Donanım Arızası	2 saat	7 gün x 24 saat
Yüksek	Servis Kesintisi (Kritik olmayan sistemlerde)	4 saat	7 gün x 24 saat
Orta	Konfigürasyon Değişiklikleri	24 saat	7 gün x 24 saat
Orta	Versiyon Güncelleme	48 saat	7 gün x 24 saat

15. İSTENEN BELGELER

15.1. Teklif Dosyasında Sunulacak Belgeler

15.1.1. İstekliler, Kamu Bilişim Yetki Belgesine sahip olacaktır. İhale dosyasında bu belge sunulacaktır.

15.2. Sözleşme İmzalama Aşamasında Sunulacak Belgeler

15.2.1. Yüklenici, TABLO 1.1 ve TABLO 1.2 ürünlerinde (Parçalı bakım ve network sorunları), Fabrikalarımızın bulunduğu en az Türkiye'nin 5 Coğrafi bölgesinin her birinde kendisine ait veya anlaşmalı Hizmet Yeterlilik Belgesine sahip 7/24 hizmet verecek kapasitede servis noktası belgesini en geç sözleşme tarihinde İdareye sunacaktır.

15.2.2. Yüklenici, Bilişim ürünleri parçalı bakım, onarım ve network ağ güvenliği hizmetleri sözleşmesinin yürürlüğü süresince, teklif verdiği ürün ile ilgili, bünyesinde gerekli görülen durumlarda ileri seviye sorunların çözümü için aşağıdaki belgelere sahip uzmanlarla destek sağlayacaktır. Bu ekipte yer alacak olan personellerde, yukarıda ilgili hizmet alımı maddelerinde de belirtildiği üzere, **teklif verdiği ürüne özel olmak koşuluyla**, aşağıda belirtilen ilgili sertifika/sertifikalar bulunacak olup, sözleşmeyi müteakip İDARE'ye sunacaktır.

15.2.2.1. En az 1 (bir) adet Broadcom Tecnicl Specialist sertifikasına sahip uzman.

TABLO 1.1 Bilişim Ürünleri ve Yan Donanımları Parçalı Bakım, Onarım Hizmeti (1 Yıllık)

Sıra No	Ürünler Yazılım ve Donanım	Adet	Birim Fiyat (TL)	Toplam Tutar Yıllık (TL)
1	Dell PE R900 (1) + R620 (1)	2		
2	Dell PE R730 (4) + R440 (19)	23		
3	FIJITSU RX300 S6 (19) Sunucu	19		
4	LENOVO SR 650	3		
5	Switch (HP(77)+Huawei(85)+Juniper(5)+SAN(2)+Dell(2))	171		
GENEL TOPLAM (TL) KDV HARIÇ				
AYLIK TOPLAM (TL) KDV HARIÇ (Genel Toplam / 12)				

TABLO 1.2 Veri Depolama ve Ağ Erişim Kontrolü Yazılımları (1 Yıllık)

Sıra No	Ürünler (Lisans, Yazılım, Donanım)	Adet	Birim Fiyat (TL)	Toplam Tutar Yıllık (TL)
1	IBM V7000 ve 7200 Veri Depolama Ünitesi	2		
GENEL TOPLAM (TL) KDV HARİÇ				

TABLO 2 Antivirüs, Antispam, Anti malware Hizmeti (1 Yıllık)

Sıra No	Ürün Adı	Adet	Birim Fiyat (TL)	Toplam Tutar Yıllık (TL)
1	Masaüstü Antivirüs Teknik Destek ve Güncelleme Hizmeti (Symantec Endpoint Security Complete SESC+DLP Lisansı)	1200		
2	Antispam Filtreleme (Mail Security) Teknik Destek ve Güncelleme Hizmeti	1000		
3	Anti Malware / İçerik Tarama ve Sandboxing Teknik Destek ve Güncelleme Hizmeti	1		
GENEL TOPLAM (TL) KDV HARİÇ				

TABLO 3 Güvenlik ve LOG Toplama Ürünleri (3 Yıllık)

Sıra No	Ürünler (Lisans, Yazılım, Donanım)	Adet	Birim Fiyat (TL)	Toplam Tutar 3 (Üç) Yıllık (TL)
1	Güvenlik Duvarı Sistemi Yenileme ve Teknik Destek Hizmeti	1		
2	WEB Koruma Yazılımı (FortiWeb WAF) Teknik Destek ve Güncelleme Hizmeti	1		
3	LOG Toplama Sistemi (SIEM) Yenileme ve Teknik Destek Hizmeti	1		
GENEL TOPLAM (TL) KDV HARİÇ				