T.C
BARTIN İL ÖZEL İDARESİ
İŞLETME VE İŞTİRAKLER MÜDÜRLÜĞÜ

TEKLİF MEKTUBU

TEKLİF SAHİBİNİN	
Adı Soyadı/Ticaret Ünvanı	.....
Tebligat Adresi	.....
Bağlı Olduğu Vergi Dairesi	.....
Vergi Numarası	.....
T.C.Kimlik Numarası	.....
Telefon No	.....
Faks No	.....
E-Mail	.....

İdaremiz ihtiyacı olan aşağıda cinsi, miktarı ve özellikleri yazılı mal alım / hizmet alım / yapım işi 4734 Sayılı Kamu İhale Kanunu'nun ilgili maddeleri gereği doğrudan temin yoluyla yapılacaktır. Söz Konusu işi KDV. hariç Kaç TL'na verebileceğiniz/yapabileceğinizi **01/03/2018 günü Saat 15:00'**a kadar kapalı zarf ile İdaremiz İşletme ve İştirakler Müdürlüğüne veya taranmış halinin bilgiislem@bartinozelidare.gov.tr e-posta adresine gönderilmesi rica olunur.

Zühal BUYURAN
İşletme ve İştirakler Müdürü

S.NO	CİNSİ , PLAKASI, MODELİ	MİKTAR	BİRİM FİYATI	TOPLAM TUTARI
1	Kurumsal Anti-Virüs Programı (120 Kullanıcılı - 1 Yıllık)	1 Adet		
	NOT: Teknik Şartname ektedir.			
			GENEL TOPLAM	

Teklif konusu işin tamamını KDV.hariç (Rakamla)..... -TL'na (Yazıyla), ... -TL.'na bedel karşılığında, teklifin teyidine müteakip, belirtilen iş günü içerisinde teslim etmeye / yapmayı, 22.11.2016 tarihli ve 29896 sayılı resmi gazetede yayımlanarak yürürlüğe giren 678 sayılı KHK'nin 30. maddesinde belirtilen hükümlere göre yapılacak araştırma sonucu talep ve ödemenin yapılacağı, aksi durumda herhangi bir hak iddia etmeyeceğimi, idaremizin çıkarına aykırı bir eylem ve oluşum içerisinde olmayacağımı,

- İdarenizin çıkarlarına aykırı bir eylem ve oluşum içerisinde olmayacağımı,
- İdare teklifde belirtilen miktarın tamamanı alıp almamakta serbestir.
- Malın/ İşin teslim süresi ..... (.....) İş günüdür.

KABUL VE TAAHHÜT EDERİM.

TEKLİF VERMEYE YETKİLİ
KİŞİ/FİRMA
ADI SOYADI-KAŞE-İMZA

TEYİT EDENİN	
Adı Soyadı =	Teyidi yapılan Mal Alımı / Hizmet Alımı / yapım işinin teyit tarihinden itibaren (.....) iş günü içerisinde teslimi yapılacaktır.
Ünvanı =	
İmzası =	
TARİH =	

T.C.
BARTIN İL ÖZEL İDARESİ

KURUMSAL ANTİ-VİRÜS GÜVENLİK PROGRAMI TEKNİK ŞARTNAMESİ

1) Program Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, Windows Server 2016 üzerinde tam uyumlu olarak çalışabilmelidir. 32 bit ve 64 bit işletim sistemleri için ayrı yükleme dosyalarına sahip olmalı ve tam uyumlu çalışmalıdır.

2) Anti-virüs programının kurulduğu bilgisayar bilgileri ayrıntılı bir şekilde merkezi bir konsoldan alınabilmelidir.

3) Program, virüs imzalarıyla tanınmayan zararlıları tespit etmek, uygulamaların istenmeyen davranışları yapmalarını kontrol edebilmek ve kayıt defteri erişimini sınırlayabilmek için Host Saldırı Önleme Sistemi (HIPS) özelliğine sahip olmalıdır.

4) Yetkisiz medya aygıtlarının sisteme takılmasını engelleyebilmeli, yöneticinin istediği aygıtlara aygıt seri numarasına bağlı olarak kullanıcılar seçilerek parametrik izinler verebilmelidir.

5) Program aygıtları depolama aygıtları, yazıcılar ve klavyeler, bellek kartı okuyucu, bluetooth olarak ayırıp buna göre izinleri ve yetkileri ayarlayabilmelidir.

6) Ağ kaynaklarını daha verimli kullanabilmek için zamanlanmış güvenlik görevlerinin belirlenen bir zaman aralığında rastgele çalıştırabilmeyi desteklemelidir.

7) Program, güncellemelerin bilgisayar üzerinde yol açabileceği olası sorunları önleyebilmek için bir sorun ya da uyumsuzluk anında eski tarihli imzalara dönebilmeyi desteklemelidir.

8) Program, zararlı yazılımları tespit edebilmek için geleneksel imzaların yanı sıra akıllı jenerik imzalar, pasif sezgisel tarama ve gelişmiş sezgisel tarama yöntemlerinin tümünü kullanan tek bir tarama motoruna sahip olmalı ve bu sayede bilinen tehditleri tespit ederken bilinmeyen tehditleri de hatalı alarm üretmeden tespit edebilmelidir.

9) Program, mevcut donanımlar üzerinde herhangi ek bir yatırım gereksinimi gerektirmeden uyumlu çalışabilmeli, minimum sistem kaynağı kullanımıyla maksimum sistem korumasını sağlayabilmelidir.

10) Programın isteğe-bağlı virüs tarama özelliği, istenildiği zaman düşük öncelikli olarak arka planda çalıştırılabilmeli böylece kullanıcı sistemde çalışırken de performans düşmeden tarama işlemi yapılabilmelidir.

11) Programın hem Türkçe hem de İngilizce sürümü bulunmalı ve aynı lisansla her iki dil sürümü de kullanılabilmelidir.

12) HTTP, HTTPS ve POP3, POP3S iletişim kuralları kullanan uygulamalarla entegre olarak bu iletişim kurallarını otomatik olarak tarayabilme özelliğine sahip olmalıdır.

13) Gelen ve giden tüm postaların taranması yaygın e-posta istemcileri Microsoft Outlook, Outlook Express, Mozilla Thunderbird ve Windows Mail ile tam entegre olarak çalışabilmelidir.

14) Programın yönetim konsolunda rol tabanlı ayrıntılı yetkiler tanımlanabilmeli ve bu yetkilere göre kullanılabilmeli ve kullanıcı aktiviteleri izlenebilmelidir.

15) Güvenlik duvarı, gerçek zamanlı koruma, web erişimi koruması ve istemci e-posta koruması gibi koruma modüllerini uzaktan etkinleştirebilmeli ve devre dışı bırakılabilmelidir.

16) Yönetim konsolünde değişik istemci özelliklerine göre değişken dinamik grup tanımları yapılabilmeli, böylece istemcilerin bu gruplara otomatik olarak eklenip çıkarılması sağlanmalıdır.

17) Program, CSV, txt, Windows olay günlüğü formatlarında günlükleri uç noktalarda saklayabilmelidir.

18) Günlüklerin ve raporlama bölümü parametreleri isteğe göre ayarlanabilmelidir.

19) Çıkarılabilir aygıtlar ile ilgili tüm eylemler Aygıt Kontrol Raporları sayesinde ayrıntılı olarak kolayca raporlanabilmelidir.

20) Program tek bir noktadan konsol ile uzaktan kurulabilmeli, kaldırılabilmeli ve yönetilebilmelidir.

21) Program tüm bileşenleri için ayrı günlük dosyaları tutabilmeli ve bu günlük dosyaları yönetim konsolundan kolayca izlenebilmelidir.

22) Geniş raporlama seçeneklerine sahip olmalı, belirli tarihler arası, istemciye göre, virüs tipine göre v.b. kriterlere göre ayrıntılı raporlar alınabilmelidir.

23) Program yönetim konsolünde istemcilerin MAC adresi de görülebilmeli ve bu sütun üzerinden işlem yapılabilmelidir.

24) Yönetim sunucusuna bağlanmak isteyen istemcilerin güvenliği için yönetim sunucusu şifre doğrulamayı desteklemeli sadece yetkili şifreye sahip istemcilerden bağlantı kabul edilebilmelidir.

25) İstemci sayısının fazlalığı ve lokasyon çokluğu ve uzaklığı durumlarında birden fazla yönetim sunucu kurup bunları birbirine replike etmeyi ve tek bir noktadan yönetmeyi desteklemelidir.

26) Ağ ortamında, ağ trafiğini korumak ve hızlı güncellemeler için merkezi tek veya birden fazla güncelleme dağıtabilme özelliğine sahip olmalıdır.

27) Kullanıcılar hard disk, flash disk ve ağ sürücüleri üzerinde virüs taraması yapabilmelidir.

28) İstenildiğinde kaldırılabilir medya sürücülerine (USB disk v.b.) erişim engellenebilmeli ve ayrıca istenen cihazlara ayrıcalık tanınabilmelidir.

29) Kullanıcı bilgisayarlar üzerinde gerçek zamanlı tarama yapan bir modül sürekli çalışmalı ve işletim sistemi çekirdeğine yapılan tüm erişimleri kontrol edebilmelidir. Hard disk, Flash disk ve diğer tüm yerel diskler üzerindeki bir dosya üzerinde yapılan her işlemi (açma, değiştirme, yazma, okuma) takip etmelidir.

30) Antivirüs programı kendi dosyalarını durdurmak ve değiştirmek isteyen zararlı yazılımlara karşı sürekli güncellenebilir bir savunma mekanizmasına sahip olmalıdır.

31) Gerçek zamanlı taramada ön tanımlı olarak tüm dosya tipleri taramaya dâhil edilmeli (Tüm sistem dosyaları, tüm sıkıştırılmış dosya formatları, tüm imaj dosya formatları, v.b.) istenirse bazı dosya tiplerinin, dosyaların ve klasörlerinin tarama dışı bırakılması sağlanabilmelidir.

32) Tarama için dosya büyüklüğü, dosya tarama zamanaşımı limitleri istenildiği gibi belirlenebilmelidir.

33) Arşiv dosyalarını taramada, sıkştırma katı ve dosya boyutu belirlenebilmelidir.

34) Güncellemeden sonra bilgisayarın kapatılıp açılma ihtiyacı olmamalıdır.

35) Kullanıcı tarafında Anti-virüs istenildiğinde "Sessiz Kip'te çalışabilmeli, antivirüs uyarıları sadece sistem yöneticisine yönlendirilebilmelidir.

36) Tarama sırasında tespit edilen virüslü dosyalar karantinaya alınabilmelidir. İstenirse karantinadan belirli bir lokasyona geri alınabilmeli ya doğrudan ya da yönetim sunucusu aracılığıyla virüs analiz laboratuarlarına gönderilebilmelidir.

37) Karantinaya alınan virüslü dosyalar özel kriptolanmış bir klasöre otomatik olarak kopyalanmalı ve bu dosya içinde durduğu süre içinde virüs aktif durumda olmamalıdır.

38) Programı esneklik ve tam sistem güvenliği açısından mobil kullanıcıların hem firma içindeyken hem de firma dışına çıktıklarında otomatik olarak güncellemeleri sağlanmalıdır.

39) Programının yönetim konsolu Windows Server 2008/2012/2016 sistemlere kurulabilmeli ve Windows tabanlı ayrı bir uygulama olmalıdır.

40) Programın yönetim konsolu ve sunucusu verilerini Microsoft Access, Microsoft SQL Server, MySQL Server ve Oracle database lerin tamamında saklayabilir olmalıdır.

41) Programın yönetim konsolundaki Politika Yöneticisi (Policy Manager) aracılığıyla hiyerarşik politikalar (policy) tanımlanabilmeli, bu politikalar istenilen grup, kullanıcıya uygulanabilmeli, oluşturulan politikalar istenildiğinde Politika Yöneticisi (Policy Manager) aracılığı ile birleştirilebilmeli.

42) Programının yönetim konsolundan ağ içerisindeki kullanıcıların antivirüs yazılımı ayarlamaları ister ayrı ayrı, ister gruplar halinde yapılıp, ilgili kullanıcılara dağıtılabilmelidir.

43) Anti-virüs Programının tutacağı log süreleri ve boyutları kullanıcı tarafından belirlenilebilmelidir.

44) Anti-virüs programı istemcisi, ajan (agent) olmamalı, gerektiğinde lisans bilgileri girilerek yerel sunucudan bağımsız olarak çalışabilmelidir.

45) Anti-virüs programı istenirse, gelen ve giden maillerin altına, mailin hangi virüs imza veri tabanı ile tarandığını ekleyebilmelidir.

46) Anti-virüs yönetim konsolundan uzaktan yükleme yapılabildiği gibi kaldırma işlemi de desteklenmelidir.

47) Anti-virüs yönetim konsolu istemci makinelerin grup bilgilerini active directory içerisinden alabilmelidir.

48) Anti-virüs yönetim konsolu aynı kuruma ait birden fazla lisansı yönetimsel olarak kullanabilmelidir.

49) Anti-virüs Programı ile ilgili teknik destek ücretsiz, Türkçe ve yurtdışı kaynaklı olarak İngilizce verilebilmelidir.

NOT1: Teknik şartnameye asgari düzeyde uygun marka bağımsız tüm güvenlik yazılımları teklif edilebilir, ancak teklif edilen ürünün teklifle birlikte bildirilmesi gerekmektedir. Teklif edilen ürün, İdaremiz muayene kabul komisyonunca teknik şartnameye ve mevcut sistemimize uygunluğu incelendikten sonra kabul edilecektir.

NOT2: İdaremizin herhangi bir ürün için herhangi bir firmayı "register" olarak kayıt etme/önerme gibi bir durumu bulunmamaktadır. Bu gibi durumlar İdaremiz tarafından onaylanmamakta olup, tamamen dağıtıcı firmanın sorumluluğundadır.