**T.C.**
**ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ**
**REKTÖRLÜĞÜ**
**İdari ve Mali İşler Daire Başkanlığı**

Sayı : 19207542-934.01/ 16/06/2020

Konu : Teklife Davet

Sayın :

Kurumumuzun ihtiyacı olan (1) kalem ANTİSPAM YAZILIMI LİSANS YENİLEME işi satın alınacaktır. İlgilendiğiniz takdirde K.D.V. hariç fiyat teklifinizi en geç 23/06/2020 tarihine kadar göndermenizi, teklifinizde teslimat süresinin de bildirilmesini rica ederim.

Ali KANBER
Satınalma Şube Müdürü

Satınalma tarih ve saati : 23/06/2020 - 10:00
Teklif Başvuru Yeri : Eskişehir Osmangazi Üniversitesi Rektörlüğü İdari ve Mali İşler Daire Başkanlığı Meşelik Kampüsü/ESKİŞEHİR

Teslimat Yeri : Eskişehir Osmangazi Üniversitesi Rektörlüğü Depoları Meşelik Kampüsü-ESKİŞEHİR

Teklif Türü : Teklif Birim Fiyat - İşin tamamı

## İhtiyaç Listesi

| Sıra No | Malın / İşin Adı | Miktar | Birim | Birim Fiyat | Tutar |
|---|---|---|---|---|---|
| 1 | ANTİSPAM YAZILIMI LİSANS YENİLEME (1 YILLIK) | 1 | ADET | | |

EK: Teknik şartname

Satınalmanın Yapılacağı Birim: ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ
NOTLAR:
1) Teklif mektupları üzerinde sipariş sonrasında ürünlerin kaç günde teslim edileceği belirtilecektir.
2) Teklif zarfları elden, posta veya faks yolu ile tarafımıza gönderilecektir.
3) Teklif edilen malzemelere ait orijinal katalog var ise teklif mektupları içerisinde getirilmesi gerekmektedir.
4) Şartlı teklifler ve Türk Lirası haricinde verilen fiyatlar değerlendirmeye alınmayacaktır.
5) Teklif edilen ürünlerin marka ve modelleri teklif mektubunda ayrıntılı olarak belirtilecektir.
6) Teklifler KALEM bazında değerlendirilecektir.
7) İSTEKLİLER VERGİ NO/TC NUMARALARINI MUTLAK SURETLE BELİRTECEKLERDİR.

Meşelik Kampüsü ESKİŞEHİR
Telefon: (222) 2393750-5505-5506 Faks: (222)2290056 e-posta: esogusatinalma@ogu.edu.tr Elektronik ağ: www.ogu.edu.tr

# ANTI-SPAM AĞ GEÇİDİ

# TEKNİK ŞARTNAME

1. Teklif edilecek e-posta güvenlik sistemi, kendi işletim sistemi ile birlikte software appliance veya virtual appliance kurulum paketlerini içermelidir.
2. Teklif edilecek eposta güvenlik sistemi limitsiz domain lisanslamayı desteklemeli, domain sayısına veya email tarama rakamlarına göre lisanslama modeli olmamalıdır.
3. Teklif edilecek eposta güvenlik sisteminin lisanslaması 24 saat esasına göre üzerinden geçen gerçek mail adreslerinin 5 günlük ortalamasına göre yapılabilmelidir. Lisans aşımı yapıldığında yöneticiyi email ve web arayüzde popup pencere ile uyarmalıdır.
4. Lisans bilgileri ve kullanımı web arayüzünde görülebilmeledir.
5. Teklif edilecek eposta güvenlik sisteminde lisans aşımı olduğunda lisans süresince bir üst pakete lisans farkı ödenerek upgrade sağlanabilmeli.
6. Teklif edilecek eposta güvenlik sistemi, email sunuculardan bağımsız olarak çalışmalıdır. MTA (Mail Transfer Agent) olarak çalışabilmelidir.
7. Eposta güvenlik sistemi HTTP proxy ayarlarını desteklemelidir.
8. Eposta güvenlik sisteminde IPV6 desteği bulunmalıdır.
9. Eposta güvenlik sisteminde birden fazla ethernet desteği olmalı ve static route, port forwarding, ip adress alias tanımlamaları yapılabilmelidir.
10. Eposta güvenlik sistemini sürüm güncellemeleri otomatik zamanlanabilmeli, indirilen güncelleme sürümü için uyarı maili gönderebilmelidir. Sistem yöneticisi sürüm güncellemesinin teknik ayrıntılarını inceleyebilmeli ve istediği zaman upgrade işlemini elle başlatabilmeledir.
11. Eposta güvenlik sistemi VMware ve Virus Bulletin sertifikalarına sahip olmalıdır.
12. Yazılımın Vmware, ISO, AWS C2 ve Azure kurulum kalıpları mevcut olmalıdır.
13. Spam tespit oranı %99,7 altında, False Positive oranı ise %0.03 den fazla olmamalıdır.
14. Eposta güvenlik sistemi Outlook Add-in yazılımına sahip olmalı ve ekstra maliyet yükü oluşturmadan Outlook 2007/2010/2013/2016 sistemlere kurulabilmeledir. Bu yazılım ile HAM veya SPAM işaretlemeyi destekleme ile otomatik öğrenmeye kullanıcılar tarafından desteklenebilmelidir.
15. Eposta güvenlik sistemi System Health Check özelliğine sahip olmalıdır, tek tıklama ile tüm sistemdeki koruma modüllerinin sağlık kontrolü sağlanabilmeledir.
16. Eposta güvenlik sistemi web arayüzden shutdown/restart özelliklerine sahip olmalı, web arayüze erişimin mümkün olmadığı durumlarında komut konsolundaki seçeneklerden bu işlemler sağlanabilmelidir.

Mehmet KOÇ
Bilgisayar Mühendisi

Ahmet GÜRLEK
Elektronik Yüksek Mühendisi

17. Eposta güvenlik sisteminin web arayüzünde dashboard bölümü bulunmalı, dashboard sistem yöneticisini grafiksel ve istatiksel özet verileri sunabilmeli, dashboard ekranında sistem kaynak bilgileri ve canlı kuyruk trafik verileri görülebilmelidir.
18. Eposta güvenlik sistemi güvenli uzaktan destek port sistemini desteklemeli, bu özellik sayesinde sistem yöneticisini sorun durumunda kompleks işlemlerle uğraşmadan üretici veya sorumlu firmaya remote bağlantı tüneli açabilmelidir.
19. Eposta güvenlik sistemi lisanslama kapsamında cluster yapıyı desteklemeli, cluster kümeler aralarında SSL veya SSL siz haberleşme sağlayabilmelidir. Kümelerin üyeliği gizli anahtar ile sağlanabilmelidir.
20. Eposta güvenlik sisteminin tüm logları (mail,message,interface) canlı olarak görüntülenebilmeli ayrıca bu logları elle dışarı çıkarma yada web arayüzden belirlediğimiz kriterlerde arama sağlanabilmelidir.
21. Eposta güvenlik sistemi Spam Test özelliğine sahip olmalı, html format veya outlook ileti dosyası elle upload ile spam kurallarından geçirilerek spam puanı test edilebilmelidir.
22. Temiz (Clean) olarak eposta sunucusuna iletilen epostalar maximum 31 gün boyunca arşivlenebilmelidir.
23. Eposta güvenlik sisteminin ayarları elle import/export edilebilmeli ve isteniliğinde yedekleme zamanlaması planlanarak otomatik belirtilen FTP adresine yedekleme sağlanabilmelidir.
24. Eposta güvenlik sistemi Remote SysLog özelliğine sahip olmalı, Mail, Interface ve Message gibi kategorilerde ayrı ayrı remote log devreye alınabilmelidir.
25. Eposta güvenlik sistemi giden mailler için Disclaimers (Hukuki alt bilgi) TEXT/HTML mesaj eklenebilmelidir. Her domain için ayrı mesaj girilebilmeli ve bazı gönderici adresler alt bilgi istisna listesine eklenebilmeledir.
26. Eposta güvenlik sistemi SNMP Management desteğine sahip olmalıdır.
27. Eposta güvenlik sistemi Global Blacklist ve Whitelist özelliğine sahip olmalı, domain ve email adres listeleri elle ve txt/csv formatında dosyadan aktarmayı desteklemelidir.
28. Güvenilir göndericiler ve kara liste tek kullanıcı (white@xyz.com) veya (@xyz.com) şeklinde ayrı ayrı düzenlenebilmelidir.
29. Eposta güvenlik sisteminde Greylisting özelliği olmalıdır. Açık veya kapalı yapılabilmeli süre ve otomatik whitelist sayısı editlenebilir olmalıdır. Ayrıca istisna göndericiler tanımlanabilmelidir.
30. Eposta güvenlik sistemi Pattern Filter özelliğini sahip olmalı, blacklist ve whitelist şeklinde pattern kuralları oluşturabilmeli, pattern filter kuralları subject, header ve body gibi özellikleri desteklemelidir.

Mehmet KOÇ
Bilgisayar Mühendisi

Ahmet GÜRLEK
Elektronik Yüksek Mühendisi

31. Eposta güvenlik sistemi NTP (Ağ Zaman Protokolü) server desteğine sahip olmalı, birden fazla sekronize sunucu adresi eklenilebilmelidir.
32. Eposta güvenlik sistemi kompleks ağ yapıları için static routes desteğine sahip olmalıdır.
33. Eposta güvenlik sistemi Recipient Verification (kullanıcı doğrulama) özelliğine sahip olmalı ve LDAP, Dynamic, Specify Allowed Receipent ve Specify Regular Expression seçeneklerini desteklemelidir.
34. Eposta güvenlik sistemi RBL (Real-time Blackhole List) kontrolü yapabilmeli, birden fazla RBL sunucu eklenebilmelidir.
35. Eposta güvenlik sistemi RBL kontrolü Recipient Verification (kullanıcı doğrulama) önce veya sonra çalışacak şekilde ayarlanabilmeli ve istenildiğinde RBL kontrol haricinde tutulabilmesi izinli IP adres yada IP adres blokları tanımlanabilmelidir.
36. Eposta güvenlik sistemi Blacklisted IP Address (Karaliste IP adresi) veya Whitelisted IP Address(Beyazliste IP adresi) özelliğini barındırmalı, istenildiği kadar IP adresi tek tek veya IP adres bloğu olarak eklenebilmelidir.
37. Sender Policy Framework (SPF) kontrol özelliğine sahip olmalı, istenildiğinde domain bazlı etkinleştirme veya devre dışı bırakılabilmelidir. Ayrıca bazı IP adreslerini veya bloklarını tarama dışı bırakma özelliği bulunmalıdır.
38. Blacklisted Top Level Domains (TLDs) özelliği bulunmalı, .info, .biz, .ru vb.gibi uzantılar listeye eklenerek email gelmesi istenilmeyen domainlerin kontrolü sağlanabilmelidir.
39. Eposta güvenlik sisteminin Relay ayarlarında güvenli hostname, güvenli network adresler tanımlanabilmelidir. Tanımlanan adreslerin relay geçişine izin verilebilmelidir.
40. Eposta güvenlik sistemi Smart Host özelliğine sahip olmalı, smart host ayarları TLS ve authentication desteğine sahip olmalıdır.
41. Yazılımın web arayüzü birden fazla dili desteklemeli özellikle Türkçe dil desteği olmalıdır.
42. Eposta güvenlik sistemi Hide Internal IP addres özelliğine sahip olmalıdır.
43. Eposta güvenlik sistemi gelişmiş routing özelliğini sahip olmalı göndericiye göre smarthost sunucu ve port bilgileri değiştirilebilmelidir
44. Gelen iletilerde DKIM kontrolü, Giden iletilerde ise domain bazlı DKIM imzalamayı desteklemeli, istenildiğinde domain bazlı açma kapatma mümkün olmalıdır.
45. Eposta güvenlik sistemi TLS Encryption desteğine sahip olmalı, bu özelliği tüm domainler veya belli domainler için kullanabilme esnekliğine sahip olmalıdır.
46. SMTP/SASL Authentication desetği bulunmalı, LDAP/Active Directory senkronizasyon sağlanarak dışarıdaki mobil POP kullanıcıların geçişine izin verilebilmelidir.
47. Eposta güvenlik sistemi Max message size (maks. mail boyutu) limitleme özelliğine sahip olmalıdır.

Mehmet KOÇ
Bilgisayar Mühendisi

Ahmet GÜRLEK
Elektrik Elektronik Yüksek Mühendisi

48. Eposta güvenlik sistemi SMTP seviyesinde RFC Compliance, Reject Unknown Sender Domain, Require Fully Qualified Domain Names, Require Fully Qualified Hostname ve Require Resolvable Hostname kontrollerini sağlayabilmeli ve istenildiğinde bu özellikler AÇIK/KAPALI yapılabilmelidir.
49. Eposta güvenlik sisteminde HELO Hostname özelliğine izinli ve engelli hostname adresler eklelenebilmelidir.
50. Eposta yazılımı kurum içerisinde bulunan bir veya birden fazla email sunucuda barındırılan domainlere gelen tüm emailleri giriş noktasında tarayabilmeledir. İstenildiğinde mail sunuculara smart host tanımlanarak giden emaillerinde taranması sağlanabilmelidir.
51. Eposta güvenlik sisteminin yönetimi web arayüz ile yapılabilmeli, erişim HTTP veya HTTPS protokolleri ile sağlanabilmelidir.
52. Gelen ve giden e-mailler, Bitdefender ve ClamAV olmak üzere iki farklı antivirüs motoru ile taranmalı. istenildiğinde virüs tarama motorlarından biri veya ikisi devre dışı yapılabilmelidir. Antivirüs motorlarının güncellemesi mevcut lisans bedeline dahil olmalı ayrıca lisans bedeli istenmemelidir.
53. Gelen ve Giden emaillerin eklerindeki Microsoft Office dosyalarında OLE2 tespiti yapabilmeli, tespit olması durumunda Spam yada Virüs olarak eylem ayarlanabilmelidir.
54. Gelen ve giden emailler anti-spam ve ek dosya uzantı kontrolünden geçişi sağlanabilmelidir.
55. Email güvenlik sistemi gelişmiş API desteğine sahip olmalıdır. API kullanımı sadece izin verilen IP adresleri için geçerli olmalıdır. API entegrasyonu kolay olmalı domain yönetimi, karantina yönetimi, beyaz liste, karaliste vs. gibi işlemleri yapabiliyor olmalıdır.
56. Anti-spam, virüs ve ek dosya uzantı kontrol ayarları gelen ve giden emailler için ayrı ayrı yapılabilmeledir. İstenildiğinde giden emaillerde ek dosya uzantı kontrolü kapatılabilmeli yada anti-spam ve virüs kontrolleri devre dışı yapılabilmelidir.
57. İstatiksel ve grafiksel özet zamanlanmış raporlar tanımlanabilmeli, bu raporlar excel, pdf veya text formatında belirlenen eposta adreslerine otamatik gönderilebilmelidir.
58. Zamanlanmış raporlar aynı zamanda sistem üzerinde arşivlenebilmelidir.
59. Istenildiğinde elle istatiksel ve grafiksel özet raporlar oluşturabilmelidir. Bu raporları yönetici pdf, excel veya text formatında dışarı çıkarabilmeledir.
60. İşlemden geçen mailler, CPU, RAM ve virüs saldırılarının sonuçlarını günlük, haftalık, aylık ve yıllık bazda grafiksel özet raporlar tek bir ekranda gösterilebilmelidir.
61. Rate control özelliği olmalı. SMTP bağlantıları ve mesajlar süre/sayı olarak limitlenebilmelidir.

Mehmet KOÇ
Bilgisayar Mühendisi

Ahmet GÜRLEK
...ktrik Elektronik Yüksek Mühendisi

62. Kural tabanlı rate contol özelliği olmalı, kaynağa/hedefe göre belli sürede mesajın boyutu veya sayısına göre kurallar oluşturabilir olmalı eylem olarak reject veya erteleme gibi eylemler tanımlanabilmelidir. Ayrıca oluşturulan kurallarda önceliklendirme yapılabilmeli çakışan kurallar olursa kuralın devre dışı kalması sağlanabilmelidir.
63. Rate limit politikasındaki eylemlerde sistem yöneticisini bilgilendirmek için email uyarı sistemi olmalıdır.
64. Eposta güvenlik sisteminde header, body veya ekine göre özel filtrelemeler yapılabilmelidir.
65. Eposta güvenlik sisteminden geçen mail trafiğinin geçmiş kayıtlarını konuya, kaynak IP adresine, gönderici adresine, spam puanına, alıcıya göre filtrelemesi kolay ve esnek bir şekilde yönetilebilmelidir. Mail trafik takibi kolayca raporlanabilmeli istenilen filtreleme sağlandıktan sonra bu veriler dışarıya export edilebilmelidir.
66. Domain karantina yöneticisi tanımlanabilmelidir. Sistem yöneticisi karantinadaki bir maili öncelikle karantina yöneticisine yönlendirebilmeli, geçişini sağlayabilmeli yada izinli listesine ekleyebilmelidir.
67. Karantina bakım periyodu günlük olarak ayarlanabilmelidir.
68. Ürünün arayüzünde kurum logosu kullanmayı desteklemeli, görsel tema ve yazı renkleri özelleştirilebilir olmalıdır.
69. Karantina rapor ayarları sistem yöneticisi tarafından ayarlanabilmeli, rapor ayarlarında gönderici adres, konu , logo, rapor oluşturma saati vb. gibi kısımları editlenebilmelidir.
70. Karantina raporları birden fazla dili desteklemeli, dil desteklerinde Türkçe seçenek bulunmalıdır. Kullancıya gönderilecek karantina raporları tamamen Türkçe ve basit anlaşılır şablonda olmalıdır.
71. Kullanıcı kendisine gelen rapor iletisindeki listede iletme, beyaz listeye ekleme veya silme işlemlerini yapabilmeli yada ayarlanan saatin dışında her hangi bir zamanda yeni bir rapor talep edebilmellidir.
72. Karantina LDAP, POP3, SQL, IMAP gibi alternatifli otantikasyon yöntemlerini destekleyerek kullancıların web arayüzden karantina listelerine ulaşması sağlanabilmeledir. Kullanıcılar karantina listelerde silme, iletme ve beyaz liste oluşturma yapabilmeli, kendine ait beyaz/kara liste domain email adres listeleri ekleyebilmelidir.
73. Eposta güvenlik sisteminin XML tabanlı API entegrasyonu desteklemelidir.
74. Eposta güvenlik sisteminin spam tarama motoru Bayesian Analysis, Auto Learning, OCR Scan, Botnet Analysis, OS Fingerprint detection, Penpals Soft, Tuning ve Network Test gibi fonksiyonlara sahip olmalı ve bu ayarlar yönetici tarafından AÇIK/KAPALI yapılabilmeli ayrıca özel değerler verilebilmelidir.

Mehmet KOÇ
Bilgisayar Mühendisi

Ahmet GÜRLEK
...ik Elektronik Yüksek Mühendisi

75. Spam, Virüs, Attachment kontrollerini domain veya kullanıcı bazlı yapılabilmelidir.
76. Grup domain veya belli domain adresine global yasaklama listesinin dışında özel attachment filter listesi uygulanabilmelidir.
77. Son 24 saat içinde Top 10 virüs ve spam relay yapan IP adreslerini otomatik olarak blacklist adres listesine ekleme özelliği olmalı, gerektiğinde UI den kapatmak mümkün olmalıdır.
78. Bir alıcı SMTP sunucu göndericiyi doğrulamak istediğinde istemciden sertifika isterse Spam Gateway sertifika göndermeyi desteklemeli istenildiğinde bu özelliği UI den açmak ve kapatmayı desteklemelidir.
79. Anti-Spoofing kontrol özelliği olmalı, bu özelliği domain bazlı açıp / kapatmak mümkün olmalıdır.
80. Karantina email raporları kullanıcı veya domain bazlı yapılabilmelidir.
81. Karantina email raporlarında spam puan kriteri belirtilebilmeli, belirtilen puan üstündeki mailler gönderilen rapor maillerine dahil edilmeyecek böylelikle kullanıcı spam oranı çok yüksek olan gereksiz kabarık liste karşılaşmamalı
82. Karantina spam için taban ve tavan puanları her domain veya kullanıcı için sistem yöneticisi tarafından belirlenebilmelidir.
83. Her domain veya kullanıcı için ayrı ayrı karantina eylemleri belirlenebilmelidir. Eylemler arasında TAGGED, REJECTED, QUARANTINED seçeneklerine sahip olunmalıdır.
84. Domain admin ve sistem admin ayrı ayrı gruplandırılabilmelidir.
85. Her domain için birden fazla domain yönetici adresi tanımlanabilmelidir. Domain yöneticileri kendi domain ve kullanıcıların ayarlarını değiştirebilmelidir.
86. Önerilen tüm yazılımlar ile veritabanı ve uygulama yazılımları firma tarafından ücretsiz olarak kurulacak ve çalışır durumda teslim edilecektir.
87. Yazılım Türkçe karakter setini desteklemelidir.
88. Teknik destek Türkçe verilmeli, Satın alınan yazılımın teknik destek ve dokümanları için ek ücret talep edilmeyecektir.
89. Yüklenici firma tarafından şartname de bahsi geçen yazılım için sağlanacak destek, Lisans süresi boyunca, telefon ve e-posta olarak mesai saatlerinde sınırsız olarak sağlanmalıdır.
90. Yazılımın sürüm geçişleri, lisans süresi boyunca ücretsiz yapılmalıdır.

Mehmet KOÇ
Bilgisayar Mühendisi

Mehmet GÜRLEK
Elektrik Elektronik Yüksek Mühendisi