

T.C.  
AYDIN BÜYÜKŞEHİR BELEDİYESİ  
SU VE KANALİZASYON İDARESİ GENEL MÜDÜRLÜĞÜ



# ASKİ

T.C.  
AYDIN BÜYÜKŞEHİR BELEDİYESİ  
SU VE KANALİZASYON İDARESİ GENEL MÜDÜRLÜĞÜ  
BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI

AĞ GÜVENLİK YAZILIMI LİSANSI ALIM  
TEKNİK ŞARTNAMESİ

- 2023 -

**İşin Sahibi** : T.C. Aydın Büyükşehir Belediyesi Su ve Kanalizasyon İdaresi Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı

**İşin Adı** : Ağ Güvenlik Yazılımı Lisansı Alımı

## TANIMLAR

Bu şartnamede;

Bilgi İşlem Dairesi Başkanlığı: **İdare**

İşi yapmaya aday gerçek veya tüzel kişi: **İstekli**

İşi yapmaya hak kazanacak gerçek veya tüzel kişi: **Yüklenici**

## A- İŞİN TANIMI

İşbu Teknik Şartname, Aydın Su ve Kanalizasyon İdaresi Genel Müdürlüğünde kullanılmakta olan sunucu, istemci, taşınabilir bilgisayar ve mobil cihazların ağ güvenlik yazılımı lisansı alımına ait teknik özellik ve hususları kapsar.

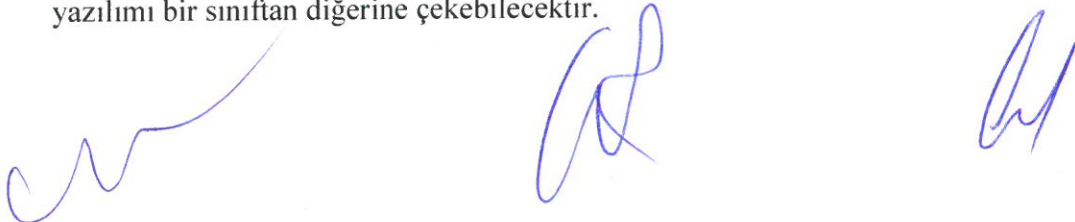
## B- GENEL HUSUSLAR

1. Satın alınacak Ürün, Yüklenici tarafından İdarenin tüm sunucu, istemci, taşınabilir bilgisayarlara yüklenmiş ve çalışır vaziyette teslim edilecektir.
2. Ürün bulutta Merkezi Yönetim Paneli ile yönetilebilecek, yedeklenebilir, 7/24 erişim sağlanabilecek ve üretici firma garantisinde olacaktır.
3. Satın alınacak her bir mal ve hizmete ait orijinal belge ve döküman (İngilizce ve/veya Türkçe) tam olarak kullanıcıya teslim edilecektir.
4. Yüklenicinin teslim edeceği ürün fiyatları, İdare'nin göstereceği adrese teslim fiyatlarıdır. Her türlü nakliye, navlun, sigorta, gümrük ve benzeri maliyetler dâhil fiyatlardır ve Yüklenici tarafından karşılanacaktır. Yüklenici, resmi teklifinde belirtmiş olduğu Ürün fiyatları haricinde başka hiçbir koşul veya isim altında bedel talep etmeyecektir.
5. Ürün teslim süresi, sipariş tarihinden itibaren en fazla 3 haftadır. Ancak kanunlarda belirtilen mücbir sebeplerden dolayı teslim süresinin uzaması durumunda taraflar yeni teslim tarihi belirleyecektir. Mücbir sebep halleri dışındaki gecikmeler, cezaya tabidir.
6. Ürünle birlikte sağlanan lisanslar İdare adına kayıtlı ve son sürüm olmalı veya son sürüm Yüklenici tarafından en geç teslimattan sonraki 1(bir) hafta içinde İdare onayıyla yüklenmelidir.
7. Ürünün belirtilen sürede teslim edilmemesi veya teklif edilen ve onaylanan üründen farklı model/nitelikte getirilmesi durumunda, oluşacak zarardan dolayı İdarenin uğrayacağı maddi ve manevi tazminatlar Yüklenici tarafından kayıtsız şartsız kabul edilecektir.

## C- AĞ GÜVENLİK YAZILIMI

### 1. Merkezi Yönetim Konsolu

- 1.1. Merkezi yönetim konsolu, herhangi bir işletim sistemi lisansı gerekiyorsa dahil olacak şekilde sunulacaktır.
- 1.2. İşletim sistemi lisansı İdare adına kaydı oluşturulacaktır.
- 1.3. Merkezi yönetim konsoluna HTTPS üzerinden güvenli bağlantı kurulabilir olacaktır.
- 1.4. Merkezi yönetim konsolundan, istemcilerin donanım bilgileri, IP adresleri, işletim sistemleri kolayca görüntülenebilecektir.
- 1.5. Merkezi yönetim konsolu ile bağlı istemcilerin güvenlik uygulama ayarları tek tek ya da gruplar halinde ilkeler yardımıyla yapılabilecektir.
- 1.6. Merkezi yönetim konsolu Microsoft Active Directory istemcilerini görüntüleyebilecek veya bunun için yardımcı yazılımları ücretsiz olarak barındıracaktır. Grup politikaları aracılığı ile kurulum scriptleri sunabilecektir. Microsoft Active Directory üzerinden kullanıcı ve grup yapısını çekebilecektir. Bu bağlantı için, direk olarak Active Directory sunucusuna bağlanabileceği gibi, görevlendirilmiş başka uç noktalar üzerinden de bu verinin merkezi yönetim sunucusuna aktarımını sağlayabilecektir.
- 1.7. Merkezi yönetim konsolu, eposta adresleri aracılığıyla sistem kullanıcıları tanımlayabilecek, bu kullanıcılara en az 5 adete kadar cihaz atayabilecek, bu cihazların sisteme otomatik eklenmesi için gereken yazılıma ait linkleri eposta aracılığıyla gönderebilecektir.
- 1.8. Merkezi yönetim konsolu, kullanıcıların sisteme erişimlerini kısıtlayabilmeli, rol tabanlı erişim sunabilecektir.
- 1.9. Merkez yönetim konsolu, android, apple, mac ve windows tabanlı uç nokta cihazlarını tek bir merkezden yönetebilecek, bunlara gruplarına göre politikalar atayabilecektir.
- 1.10. Merkez yönetim konsolu üzerinde, tüm istemciler üzerinde tespit edilmiş zararlı yazılımlar görüntülenebilecektir. Ayrıca, çalıştırılmış tüm yazılımlar 'Güvenilir, Zararlı ve Bilinmeyen' olarak sınıflandırılmış şekilde görüntülenebilecek, yönetim istenirse bir yazılımı bir sınıftan diğerine çekebilecektir.





- 1.11. Merkez yönetim konsolu, mac, android ve Windows tabanlı işletim sistemleri üzerinde istendiği zaman virüs taraması ve virüs veri tabanı güncellemesi başlatabilecektir. Bu tarama ve güncellemeler aynı zamanda merkez konsolu politikaları aracılığıyla zamanlanabilir olacaktır.
- 1.12. Merkez yönetim konsolu, android ve apple mobil cihazları için yazılım deposu oluşturabilecek, bu depolara kurum kendi mobil yazılımlarını koyabileceği gibi işletim sistemi üreticisinin depolarından (app store, google play) da yazılımlar tanımlanabilecektir. Kurum yazılımlarının yönetilen mobil cihazlara uzaktan yüklenmesi sağlanabilecektir.
- 1.13. Merkez yönetim konsolu, yönetilen Windows işletim sistemli cihazlarda yama kontrolü yapabilmeli, eksik işletim sistemi yamalarının yüklenmesini sağlayabilecektir. MSI uzantılı yazılımları uzaktan kurdurabilecektir.
- 1.14. Merkez yönetim konsolu, yönetilen Windows işletim sistemli cihazların tümünde çalıştırılmış yazılımların envanterini toplayabilecek, bu yazılımlar arasından istediklerini tüm kurum cihazlarında tek bir merkezden yasaklayabilecek veya güvenilir olarak işaretleyebilecektir.
- 1.15. Merkez yönetim konsolu, yönetilen mobil cihazların tümünde çalıştırılmış yazılımların envanterini toplayabilecek, bu yazılımlar arasından istediklerini tüm kurum cihazlarında tek bir merkezden yasaklayabilecektir.
- 1.16. Merkez yönetim konsolu, yönetici erişimi açılmış (rooted veya jailbroken) mobil cihazları raporlayabilecek, istenen mobil cihazlardaki kurum yazılımlarının kaldırılması emrini verebilecektir.
- 1.17. Merkez yönetim konsolu, istenen mobil cihazlarda siren çalmasını sağlayabilecek (hırsızlık veya kayıp anında destek için), ekran erişimine şifre koyabilecek veya var olan şifreyi değiştirebilecek ve kullanıcıya mesaj gönderebilecektir.
- 1.18. Merkez yönetim konsolu, üreticinin analiz laboratuvarları ile entegre olarak davranışsal analiz yapabilecek, elle kontrol istenirse ek lisans ile uzman kontrolü ve raporu için bilinmeyen yazılımı otomatik olarak analize gönderebilecektir. Analiz laboratuvarları tarafından tespit edilecek tüm zararlı, zararsız yazılımlar ve bu yazılımların yaptığı tüm aksiyonlar ile ilgili raporlar alınabilecektir. İstenirse analiz laboratuvarları entegrasyonu politika bazında kapatılabilecektir. İstenirse analiz laboratuvarları kontrollerinin kurum beyaz listelerine yazılımı güvenilir olarak eklemesi sağlanabilecektir.

**1.19.** Merkezi Yönetim Konsolu üzerinde, profil bazında alarmlar tanımlanabilecek, bu alarmlar bir veya birden fazla kriterin birleşimi olarak yaratılabilecektir. (örneğin CPU kullanımının 3 dakika boyunca 80% üzerinde olması ve/veya network kullanımının 80% den 3 dakika boyunca fazla ve/veya sistem diskinde belirli bir orandan daha az boş yer kalması ve/veya belirli bir servis/prosesin çalışmaması/çalışması, belirli bir adresin belirli bir portuna belirli bir süre ulaşılabilmesi vs durumunda alarm çalışması)

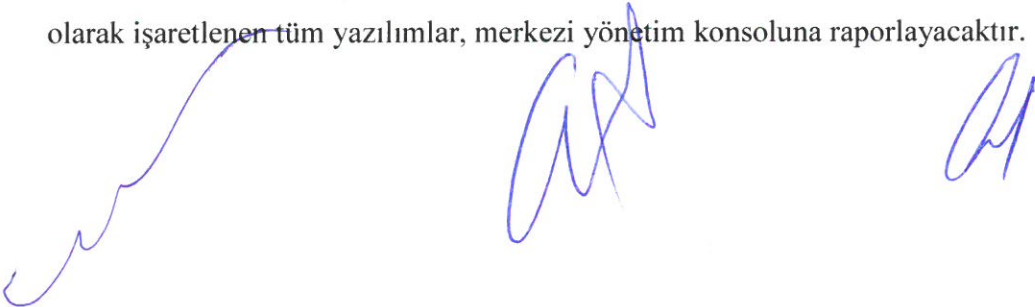
**1.20.** İstenirse alarm çalışması durumunda, istenirse de belirli zamanlarda tekrarlanabilecek şekilde uç nokta üzerinden prosedürler çalıştırılabilecektir. Bu prosedürler, programlanabilir bir yapıda olmalı, üretici, farklı prosedürlerin yazılması noktasında destek vermelidir. Örneğin, uç noktanın belirli bir yere bağlanıp bir dosyayı indirip onu belirli bir script ile kurması için prosedür yazılabilecektir. Bu prosedürler çerçevesinde uç noktalarda CMD ve Powershell scriptleri de çalıştırılabilecektir. Bu sayede, acil olarak istenen standart olmayan istekleri de karşılamak mümkün olacaktır.

## **2. Uç Nokta Güvenlik Yazılımı**

**2.1.** Uç nokta güvenlik yazılımı, merkezi yönetim yazılımı tarafından yönetilebilecektir.

**2.2.** Windows tabanlı uç nokta güvenlik yazılımı üzerinde en az güvenlik duvarı, antivirüs özelliği, davranışsal analiz özelliği, HIPS (host intrusion prevention), auto-sandbox özellikleri bulunacak ve bu özelliklere özgü politika yazılabilecektir.

**2.3.** Windows tabanlı uç nokta güvenlik yazılımı, antivirüs veri tabanı veya davranışsal analizlerle zararlı olarak tespit edilememiş yazılımları hem kurumun hem de üreticinin beyaz ve kara listelerinde kontrol edip, istenirse detaylı analiz için üreticinin analiz laboratuvarlarına detaylı analize gönderebilecektir. Bu yazılımları eğer beyaz ve kara listelerde de bulamamışsa, zararsız olma olasılıklarına karşın tamamen engellememeli, ancak zararlı olma olasılıklarına karşı da işletim sisteminden izole bir şekilde çalışmasını sağlayacaktır, herhangi bir veride değişiklik yapmasına izin vermeyecektir. İzole olarak çalıştırılan yazılımı üzerinde davranışsal analiz kontrolüne devam edebilecektir. Hangi koşullar altında yazılımın izole edileceği politika bazında ayarlanabilir olacaktır. Bu şekilde izole edilen veya izole edilmese dahi beyaz ve kara listeler vasıtasıyla 'tanınmayan' olarak işaretlenen tüm yazılımlar, merkezi yönetim konsoluna raporlayacaktır.





- 2.4. Windows tabanlı uç nokta güvenlik yazılımı tüm olayları günlük dosyalarında tutabilecek ve bu günlük dosyaları dışarı aktaracaktır. Ortak Olay biçimi CEF formatı destekleyecektir.
- 2.5. Windows tabanlı uç nokta güvenlik yazılımı kurulu olduğu bilgisayarda ilk yükleme, versiyon güncelleme ve ilk tarama durumları hariç yeniden başlatma ihtiyacı olmayacaktır.
- 2.6. Windows tabanlı uç nokta güvenlik yazılımı istenildiğinde uyarı ve bildirimlerin kullanıcıya gösterilmemesini sağlayacaktır.
- 2.7. Windows tabanlı uç nokta güvenlik yazılımı yalnızca çevrimdışı verilere karşı değil internet içeriğinden gönderilecek olan Java ve Active-x scriptlerine karşı da koruma sağlayacaktır.
- 2.8. Windows tabanlı uç nokta güvenlik yazılımı tarama sırasında tespit edilen zararlı yazılımları karantinaya alacak, karantinadaki dosyaları istenirse geri yükleyecek ve analiz laboratuvarına gönderecektir.
- 2.9. Windows tabanlı uç nokta güvenlik yazılımı Tam Tarama işlemi esnasında daha önceden taranmış ve tarandıktan sonra değişiklik yapılmamış dosyaları atlayarak tarama performansını en üst düzeye çıkarabilecektir.
- 2.10. Windows tabanlı uç nokta güvenlik yazılımı, uç noktalarda istenen zamanlarda 'bilinen&bilinmeyen' dosya taraması yapabilecektir. Bu tarama kapsamında, uç noktadaki çalıştırılabilir yazılımlar taranmalı, bilinmeyen dosyalar merkezi yönetim sunucusuna raporlanabilecektir.
- 2.11. Windows tabanlı uç nokta güvenlik yazılımı, cihaz kontrolü sağlayabilmeli, gruplanmış halde USB disk, yazıcı, Bluetooth cihazları, modem gibi dış cihazları profil bazında engelleyebilecektir. Profil bazında bu engellemenin dışında tutulacak cihazlar DeviceID parametresi ile tanımlanabilecektir.
- 2.12. Windows tabanlı uç nokta güvenlik ajanı vasıtasıyla yönetici uzak masa üstü bağlantısı yapıp destek verebilecektir. Bu özellik ek bir lisans gerektirmeyecektir.

### 3. Mobil Cihaz Güvenlik Yazılımları

- 3.1. Mobil cihazlarda, uzaktan harita üzerinde yer tespiti, root/jailbreak ile Yönetimi kırılmış cihazların tespiti, üzerinden cihaza reset atılması gibi özellikleri sunacaktır.
- 3.2. Android tabanlı uç nokta güvenliği yazılımı, aynı zamanda antivirüs özelliğine de sahip olacaktır.



- 3.3. Android tabanlı uç nokta güvenliği yazılımı üzerinde Kamera, Bluetooth, WIFI, Mobil ağ, GPS özelliklerini açıp kapatabilmeli, istenirse kullanıcı seçimine izin verecektir.
- 3.4. Android tabanlı uç nokta güvenliği yazılımı, bilinmeyen kaynaklardan yüklenecek yazılımların çalışmasını engelleyecektir.
- 3.5. Android tabanlı uç nokta güvenliği yazılımı, mobil cihazlar üzerinde güvenlik politikası uyarınca şifre tipi ve minimum şifre uzunluğunu belirleyebilecektir. Yöneticinin belirleyeceği belli bir sayıda yanlış şifre girilmesi durumunda, cihaz üzerindeki kurum yazılımlarının uzaktan silinmesine olanak tanınacaktır. Yöneticinin belirleyeceği belli bir sayıda yanlış şifre girilmesi durumunda, ön kameradan fotoğraf çekerek merkezi yönetim konsolu ile paylaşabilecektir.
- 3.6. Android tabanlı uç nokta güvenliği yazılımı, SAFE destekli cihazlarda roaming, USB tethering, WIFI erişim noktası, sms, mms gibi özellikleri kapatabilecektir. Cihazın giriş yapabileceği minimum WIFI güvenliği seviyesini belirleyebilecektir. Kiosk veya benzeri bir mod sayesinde, cihazın sadece belirlenen yazılımları çalıştırmasını, bu modda iken cihaz ayarlarına veya menülerine erişimin kapatılmasını sağlayabilecektir. Bir admin şifresi ile bu moddan manuel olarak çıkışa izin verecektir.
- 3.7. Android tabanlı uç nokta güvenliği yazılımı, eposta, WIFI, VPN bilgilerini merkezden çekecektir.
- 3.8. Apple IOS tabanlı uç nokta güvenliği yazılımı, parmak izi, airdrop, multiplayer oyunlar, game center, appstore dan yazılım alımı özelliklerini engelleyecektir. Yedeklemelerin şifreli olmasını zorunlu kılacaktır. Yazılım, film v.b. içeriklerde rating kontrolü ve sınırlaması yapacaktır.
- 3.9. Apple IOS tabanlı uç nokta güvenliği yazılımı Youtube, i-tunes yazılımlarını engelleyecektir. İstenirse safari yazılımını da engelleyecek veya bu yazılımda java script çalıştırılması, cookilerin kabul edilmesi gibi potansiyel açık yaratabilecek işlemleri engelleyecektir.
- 3.10. Apple IOS tabanlı uç nokta güvenliği yazılımı, Air Play üzerinde merkezden belirlenecek cihazları ekleyebilecektir.
- 3.11. Apple IOS tabanlı uç nokta güvenliği yazılımı, Air Print üzerinde merkezden belirlenecek cihazları ekleyecektir.
- 3.12. Apple IOS tabanlı uç nokta güvenliği yazılımı, eposta ayarlarını merkezden alacaktır.

- 3.13. Apple IOS tabanlı uç nokta güvenliği yazılımı, internet takvimlerine (calendar) merkezden gönderilecek bilgiler dahilinde entegre olacaktır.
- 3.14. Apple IOS tabanlı uç nokta güvenliği yazılımı, CardDAV sistemleri ile entegre olarak kurum kontaklarını çekebilecek, bu bilgi de merkezden profil bazında ayarlanabilecektir.
- 3.15. Apple IOS tabanlı uç nokta güvenliği yazılımı, VPN, WIFI, APN ayarlarını merkezi yönetim konsolundan çekebilecektir.

#### **D. Diğer Hususlar**

1. Ağ Güvenlik Yazılımı en az 3 (üç) yıllık ve en az 800 kullanıcı lisansına sahip olacaktır.
2. Yüklenici mevcutta kullanılan antivirüs ve/veya ağ güvenlik yazılımını tüm kullanıcılardan kaldırarak teklif edeceği ürünü kuracaktır.
3. Yüklenici teklif edeceği ürünü lisans süresi boyunca direk olarak üretici firma tarafından destek sağlanacak şekilde gerekli destek paketlerini dahil edecektir.
4. Yüklenici ilgili kurum yetkililerine teklif edeceği ürün hakkında kurulum sonrası eğitimlerini verecektir.
5. Yüklenici firma kurulum sonra yönetim panelinin tüm yetkilerini İdare ye teslim edecektir.
6. Yüklenici yukarıda yapmakla yükümlü olduğu hiçbir işi başka bir firmaya devredemez.
7. Yüklenici bu teknik şartnamede özellikleri tanımlanan ürünlerin tamamını eksiksiz, lisanslarının İdare adına kaydettirilmiş şekilde olması gerekmektedir.

Ahmet CENGİZ  
Bilgisayar Öğretmeni

Erhan ARSLAN  
Bilgisayar Teknikeri

Mehmet AKBAŞ  
Bilgisayar Teknikeri