საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტრო

ანტივირუსული პროგრამული უზრუნველყოფის
(სალიცენზიო გასაღების) შესყიდვის
ერთეტაპიანი გამარტივებული ელექტრონული ტენდერი

სატენდერო დოკუმენტაცია

ქ. თბილისი 2016 წელი

1. ტექნიკური დოკუმენტაცია

1.1 **საკვალიფიკაციო მოთხოვნების თანახმად, პრედენდენტმა უნდა წარმოადგინოს შემდეგი დოკუმენტები:**

1.1.1 **იურიდიული პირებისათვის:**

- საკვალიფიკაციომოთხოვნებისგარეშე

1.1.2 **ფიზიკური პირებისათვის:**

- საკვალიფიკაციო მოთხოვნების გარეშე

1.1.3 **როგორც იურიდიული, ასევე ფიზიკური პირებისათვის:**

(1) პრეტენდენტის შეთავაზება **დანართი N2**-ის მიხედვით;
(2) ფასების ცხრილი**დანართი N3**-ის შესაბამისად;

1.2 პრეტენდენტის მიერ წარდგენილი წინადადება ძალაშია სახელმწიფო შესყიდვების სააგენტოს თავმჯდომარის 2011 წლის 7 აპრილის N9 ბრძანებით დამტკიცებული „გამარტივებული ელექტრონული ტენდერისა და ელექტრონული ტენდერის ჩატარების წესის“მე-2 მუხლის პირველი პუნქტის „ჟ“, „რ“ ან „ტ“ ქვეპუნქტებით გათვალისწინებული ეტაპის დადგომამდე.

1.3 ელექტრონული გარანტიის მოქმედების ვადა უნდა განისაზღვროს: გამარტივებული ელექტრონული ტენდერის შემთხვევაში - არანაკლებ 120 კალენდარული დღით ტენდერისათვის სტატუსის „წინადადების მიღება დაწყებულია“ მინიჭების თარიღის შემდეგ.

1.4 **პრეტენდენტის მიერ სისტემაში ტექნიკური დოკუმენტაციის სახით ატვირთული უნდა იყოს:**

(1) პრეტენდენტის შეთავაზება **დანართი N2**-ის მიხედვით;
(2) ფასების ცხრილი**დანართი N3**-ის შესაბამისად;

1.5 **ფასები და ანგარიშსწორების პირობები:**

1.5.1 სატენდერო წინადადებაში საერთო ფასი გამოსახული უნდა იყოს ეროვნულ ვალუტაში, საქართველოს კანონმდებლობით გათვალისწინებული საქონლის მიწოდებასთან დაკავშირებული ყველა ხარჯისა და გადასახადის გათვალისწინებით.

1.5.2 ანგარიშსწორება მოხდება უნაღდო ანგარიშსწორებით ლარში, ფაქტიურად მიწოდებული საქონლის ღირებულების მიხედვით, შესაბამისი მიღება-ჩაბარების აქტის გაფორმებიდან **15 სამუშაო დღის განმავლობაში;**

1.5.3 დაფინანსების წყარო: **2016 წლის საბიუჯეტო ასიგნებები.**

1.5.4 წინასწარი ანგარიშსწორება არ გამოიყენება.

1.6 **მიწოდების პირობები და ვადები:**

1.6.1 მისაწოდებელი საქონელი უნდა აკმაყოფილებდეს **დანართი N4-ში** მოცემულ მახასიათებლებს;

1.6.2 მისაწოდებელის საქონლის (სალიცენზიო გასაღების) მოქმდებების ვადა უნდა იყოს **არანაკლებ 1 კალენდარული წელი მიწოდების დღიდან**

1.6.3 საქონლის (სალიცენზიო გასაღები) მიწოდება განხორციელდება: **ხელშეკრულების გაფორმებიდან 7 (შვიდი) კალენდარულ დღეში.**

1.6.4 საქონლის (სალიცენზიო გასაღები) მიწოდება უნდა განხორციელდეს შემდეგ მისამართზე: **ქ. თბილისი, ს. ეულის ქ. N3 - საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტრო.**

1.6.5 მიმწოდებელი ვალდებულია გადასცეს შემსყიდველს უფლებრივად და ნივთობრივად უნაკლო და ახალი საქონელი;

1.6.6 მიმწოდებელმა საქონლის მიწოდებისას უნდა წარმოადგინოს საქართველოს საგადასახადო კანონმდებლობით გათვალისწინებული შესაბამისი დოკუმენტაცია.

1.6.7 სატენდერო დოკუმენტაციასთან დაკავშირებული განმარტების ან/და დაზუსტების მიღება პრეტენდენტს შეუძლია შემდეგ მისამართზე: ქ. თბილისი, სანდრო ეულის ქ. N3, საკონტაქტო პირები:

ბექა ერაძე	577 222 910	beradze@moc.gov.ge
გიორგი კოპალიანი	551 971 133	gkopaliani@moc.gov.ge

1.7 დამატებითი მოთხოვნა:

ფასწარმოქმნის ადეკვატურობის დასაბუთება იმ შემთხვევაში, თუ ტენდერში ყველაზე დაბალი ფასის წინადადების მქონე პრეტენდენტის მიერ სისტემაში დაფიქსირებული საბოლოო ფასი 20%-ით ან მეტით დაბალია შესყიდვის ობიექტის სავარაუდო ღირებულებაზე, შემსყიდველი ორგანიზაცია პრეტენდენტისაგან მოითხოვს ფასწარმოქმნის ადეკვატურობის დასაბუთებას. აღნიშნულ შემთხვევაში პრეტენდენტმა უნდა უზრუნველყოს მწარმოებლის მიერ გაცემული, ქართულ ენაზე ნათარგმნი და ნოტარიულად დამოწმებული ინვოისის წარმოდგენა, რომელიც დაადასტურებს პრეტენდენტის მიერ დაფიქსირებულ ფასად ხელშეკრულებით ნაკისრი ვალდებულებების შესრულების შესაძლებლობას.

2. ხელშეკრულება სახელმწიფო შესყიდვის შესახებ

გამარტივებული ელექტრონული ტენდერი SPA_____

(პროექტი)

თბილისი ----------

ერთი მხრივ, საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტრო (შემდგომში "შემსყიდველი") წარმოდგენილი მისი მინისტრის მოადგილის ბესიკ დევდარიანის სახით და მეორე მხრივ, ---------- (შემდგომში „მიმწოდებელი") მისი დირექტორი ---------- სახით, საქართველოს მოქმედი კანონმდებლობის საფუძველზე და გამარტივებული ელექტრონული ტენდერის საშუალებით ვდებთ ხელშეკრულებას შემდეგზე:

1. წინამდებარე ხელშეკრულების საგანი

ხელშეკრულების საგანს წარმოადგენს საჯელაღსრულებისა და პრობაციის სამინისტროს საჭიროებისათვის ---------- შესყიდვა (**CPV48761000 - ანტივირუსის პროგრამული პაკეტები).**

2. შესყიდვის ობიექტი

შესყიდვის ობიექტია ----------.

3. წინამდებარე ხელშეკრულების საერთო ღირებულება

3.1. წინამდებარე ხელშეკრულების საერთო ღირებულება შეადგენს არაუმეტეს ---------- (----------) ლარს.

3.2. საქონლის ერთეულის და საერთო ფასი, განსაზღვრულია დანართში.

3.3. ამ თავის 3.2. პუნქტში აღნიშნული დანართი (------- ფურცელი) წარმოადგენს წინამდებარე ხელშეკრულების განუყოფელ ნაწილს და თან ერთვის წინამდებარე ხელშეკრულებას.

3.4. წინამდებარე ხელშეკრულების 3.1. პუნქტში აღნიშნულ თანხაში შედის საქართველოს კანონმდებლობით გათვალისწინებული ყველა შესაბამისი გადასახადი.

4. შესყიდვის ობიექტის ხარისხი, გარანტია, მიწოდების ვადა და ადგილი

4.1 მიმწოდებელი იძლევა გარანტიას, რომ საქონელი იქნება მაღალი ხარისხის, უპასუხებს წინამდებარე ხელშეკრულების პირობებს და დააკმაყოფილებს დანართით განსაზღვრულ მოთხოვნებს.

4.2 საქონლის **(სალიცენზიო გასაღები)** მიწოდება განხორციელდება: **ხელშეკრულების გაფორმებიდან 7 (შვიდი) კალენდარულ დღეში.**

4.3. საქონლის (სალიცენზიო გასაღები) მიწოდება უნდა განხორციელდეს შემდეგ მისამართზე: **ქ. თბილისი, ს. ეულის ქ. N3 - საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტრო.**

5. საქონლის მიღება-ჩაბარების წესი

5.1. საქონლის მიღება ფორმდება მიღება-ჩაბარების აქტით, რომელსაც ხელს აწერენ შემსყიდველის მხრიდან ლოჯისტიკის დეპარტამენტის წარმომადგენელი ----------, ხოლო მიმწოდებლის მხრიდან დირექტორი ან/და მის მიერ უფლებამოსილი პირი.

6. ანგარიშსწორების პირობები

6.1. მიმწოდებელთან ანგარიშსწორება განხორციელდება ეროვნულ ვალუტაში.

6.2. წინამდებარე ხელშეკრულებით განსაზღვრული შესყიდვის ობიექტის ღირებულების ანაზღაურება მოხდება უნაღდო ანგარიშსწორების ფორმით.

6.3 ანგარიშსწორების განხორციელებისათვის მიმწოდებელმა უნდა წარადგინოს წინამდებარე ხელშეკრულების 5.1 პუნქტში მითითებული მიღება-ჩაბარების აქტი, სასაქონლო ზედნადები.

6.4. ანგარიშსწორება შემსყიდველის მიერ მოხდება მიმწოდებლის მიერ ამ თავის 6.3. პუნქტით განსაზღვრული დოკუმენტაციის წარდგენიდან არაუგვიანეს **15(თხუთმეტი) სამუშაო** დღის განმავლობაში.
6.5. მიმწოდებელმა ანგარიშსწირების განხორციელებისათვის 6.3 პუნქტში მითითებული დოკუმენტაცია თუ არ წარუდგინა შემსყიდველს საქონლის მიწოდების დამთავრების მეორე დღიდან 3 (სამი) თვის განმავლობაში, მიმწოდებელი 3 (სამი) თვის გასვლის შემდეგ კარგავს მიწოდებულ საქონელზე თანხის მოთხოვნის უფლებას შემსყიდველისათვის დოკუმენტაციის წარუდგენლობის გამო.

7. მხარეთა ვალდებულებები და უფლებები

7.1. შემსყიდველი ვალდებულია:
ა) მოახდინოს ანგარიშსწორება მიმწოდებელთან წინამდებარე ხელშეკრულებით გათვალისწინებული პირობების შესაბამისად;
ბ) უზრუნველყოს უფლებრივად და ნივთობრივად უნაკლო საქონელის მიღება.
7.2. შემსყიდველს უფლება აქვს:
შეამოწმოს მიწოდებული საქონლის ხარისხის და რაოდენობის შესაბამისობა წინამდებარე ხელშეკრულებასთან და ------ დანართთან.
7.3. მიმწოდებელი ვალდებულია:
ა) მიაწოდოს შემსყიდველს წინამდებარე ხელშეკრულების ----- დანართით გათვალისწინებული რაოდენობისა და ხარისხიანი საქონელი;
ბ) დაიცვას წინამდებარე ხელშეკრულებით და ---------- დანართით გათვალისწინებული ყველა პირობა;
გ) შემსყიდველს მიაწოდოს უფლებრივად და ნივთობრივად უნაკლო საქონელი;
დ) შემსყიდველს მიაწოდოს წინამდებარე ხელშეკრულების 6.3. პუნქტში მითითებული ყველა დოკუმენტი;
ე) წინამდებარე ხელშეკრულების შესრულების პროცესში წამოჭრილ გაუთვალისწინებელ ხელშემშლელ გარემოებეთან დაკავშირებით, დაუყოვნებლივ გაუგზავნოს შემსყიდველს წერილობითი შეტყობინება შეფერხების ფაქტის, მისი შესაძლო ხანგძლივობის და გამომწვევი მიზეზების შესახებ.
ვ) მიწოდებულ საქონელზე აღმოჩენილი ნაკლი ან დეფექტი გამოასწოროს **5 სამუშაო დღის განმავლობაში.**
7.4. მიმწოდებელს უფლება აქვს:
მოსთხოვოს შემსყიდველს მიწოდებული საქონლის ღირებულების ანაზღაურება წინამდებარე ხელშეკრულებით გათვალისწინებული პირობებით;

8. მხარეთა პასუხისმგებლობა წინამდებარე ხელშეკრულების დარღვევისას

8.1.ხელშეკრულების პირობების არაჯეროვანი შესრულების შემთხვევაში, მიმწოდებელს ეკისრება პირგასამტეხლო წინამდებარე ხელშეკრულების საერთო ღირებულების **5 (ხუთი)** პროცენტის ოდენობით.
8.2 საქონლის მიწოდების ვადის დარღვევის შემთხვევაში, მიმწოდებელს ეკისრება პირგასამტეხლო ყოველ ვადაგადაცილებულ დღეზე წინამდებარე ხელშეკრულების საერთო ღირებულების **0.5** (ნული მთელი ხუთი) პროცენტის ოდენობით.
8.3. ინსპექტირებისას აღმოჩენილი დეფექტის, ნაკლის გამოსწორებისათვის ან/და შეცვლისათვის მიმწოდებელმა თუ გადააცილა წინამდებარე ხელშეკრულებით გათვალისწინებულ ვალდებულების შესრულების საერთო ვადას მიმწოდებელს ეკისრება პირგასამტეხლო ყოველ ვადაგადაცილებულ დღეზე წინამდებარე ხელშეკრულების საერთო ღირებულების **0.5** (ნული მთელი ხუთი) პროცენტის ოდენობით.
8.4. წინამდებარე ხელშეკრულებით აღებული ვალდებულების შეუსრულებლობისათვის მიმწოდებელს ეკისრება პირგასამტეხლო წინამდებარე ხელშეკრულების საერთო ღირებულების **10 (ათი)** პროცენტის ოდენობით.

9. წინამდებარე ხელშეკრულების მოქმედების ვადა

წინამდებარე ხელშეკრულების მოქმედების ვადა განისაზღვრება ხელშეკრულებაზე ორმხრივად ხელის მოწერის დღიდან **2017 წლის 31 იანვრის ჩათვლით.**

10. წინამდებარე ხელშეკრულების პირობების გადასინჯვის შესაძლებლობა

10.1 წინამდებარე ხელშეკრულების პირობების შეცვლა დაუშვებელია, თუ ამ ცვლილების შედეგად იზრდება წინამდებარე ხელშეკრულების ჯამური ღირებულება ან უარესდება წინამდებარე ხელშეკრულების პირობები

შემსყიდველი ორგანიზაციისათვის, გარდა საქართველოს სამოქალაქო კოდექსის 398-ე მუხლით დადგენილი შემთხვევებისა.

10.2 საქართველოს სამოქალაქო კოდექსის 398-ე მუხლით გათვალისწინებული პირობების დადგომის შემთხვევაში დაუშვებელია თავდაპირველად დადებული წინამდებარე ხელშეკრულების ჯამური ღირებულების 10%-ზე მეტი ოდენობით გაზრდა.

11. დაუძლეველი ძალა (ფორს-მაჟორი)

11.1. მხარეები არ არიან პასუხისმგებელნი თავიანთი ვალდებულების სრულ ან ნაწილობრივ შეუსრულებლობაზე, თუ ეს შეუსრულებლობა გამოწვეულია ისეთი გარემოებებით, როგორიცაა წყალდიდობა, ხანძარი, მიწისძვრა და სხვა სტიქიური მოვლენები, აგრეთვე ომები და საომარი მოქმედებები, თუ ისინი უშუალო ზემოქმედებას ახდენენ წინამდებარე ხელშეკრულების შესრულებაზე. ხელშეკრულების შესრულების ვადა გადაიწევს შესაბამისი დროით, გარემოებათა დასრულების შემდეგ.

11.2. ფორს-მაჟორული გარემოებების დადგომის შემთხვევაში წინამდებარე ხელშეკრულების მხარემ, რომლისთვისაც შეუძლებელი ხდება ნაკისრი ვალდებულებების შესრულება, პირველი შესაძლებლობისთანავე უნდა გაუგზავნოს მეორე მხარეს წერილობითი შეტყობინება ასეთი გარემოებების და მათი გამომწვევი მიზეზების შესახებ. თუ შეტყობინების გამგზავნი მხარე არ მიიღებს მეორე მხარისაგან პასუხს, იგი თავისი შეხედულებისამებრ, მიზანშეწონილობისა და შესაძლებლობის მიხედვით აგრძელებს წინამდებარე ხელშეკრულებით ნაკისრი ვალდებულებების შესრულებას და ცდილობს გამონახოს ვალდებულების შესრულების ისეთი ალტერნატიული ხერხები, რომლებიც დამოუკიდებელი იქნებიან ფორს-მაჟორული გარემოებებისაგან.

11.3. თუ სახელშეკრულებო ვალდებულებების მთლიანი ან ნაწილობრივი შეუსრულებლობის პირობები გაგრძელდა სამ თვეზე მეტ ხანს, მხარეებს უფლება აქვთ შეწყვიტონ წინამდებარე ხელშეკრულების მოქმედება, კომპენსაციის უფლების მოთხოვნის გარეშე.

12. წინამდებარე ხელშეკრულების ინსპექტირების პირობები

12.1. შემსყიდველი უფლებამოსილია განახორციელოს ინსპექტირება საქონლის მიწოდების პერიოდში ან შემდგომ.

12.2. ინსპექტირებისას ხილვადი დეფექტის, ნაკლის ასევე უხარისხო მოწოდებული საქონლის აღმოჩენის შემთხვევაში ინსპექტირების განმხორციელებელმა უნდა შეადგინოს ინსპექტირების აქტი და წარუდგინოს შემსყიდველს შემდგომი რეაგირებისათვის.

12.3. ვიზუალური დათვალიერების დროს, ხილვადი დეფექტის ან/და ნაკლის აღმოჩენის შემთხვევაში, შემსყიდველი ვალდებულია დაუყოვნებლივ წერილობით ან/და სატელეფონო შტყობინებით აცნობოს მიმწოდებელს აღმოჩენილი დეფექტის, ნაკლის შესახებ და მოსთხოვოს ნაკლის, დეფექტის გამოსწორება ან შეცვლა.

12.4. გამოვლენილი დეფექტის ან ნაკლის აღმოფხვრასთან და ხელახალ ინსპექტირებასთან დაკავშირებული ხარჯების ანაზღაურება ეკისრება მიმწოდებელს.

12.5. შემსყიდველის მხრიდან წინამდებარე ხელშეკრულების შესრულების კონტროლს განახორციელებს მინისტრის მიერ უფლებამოსილი პირი.

13. ხელშეკრულების შეწყვეტა

13.1 შემსყიდველს შეუძლია მთლიანად ან ნაწილობრივ შეწყვიტოს წინამდებარე ხელშეკრულება მიმწოდებლისთვის ვალდებულების შეუსრულებლობის ან არაჯეროვნად შესრულების შესახებ წერილობითი შეტყობინების გაგზავნის შემდეგ, თუ:

ა) მიმწოდებელს წინამდებარე ხელშეკრულებით გათვალისწინებულ ვადებში არ შეუძლია მთლიანად ან ნაწილობრივ წინამდებარე ხელშეკრულებით ნაკისრი ვალდებულების შესრულება.

ბ) მიმწოდებელს არ შეუძლია შეასრულოს წინამდებარე ხელშეკრულებით გათვალისწინებული რომელიმე ვალდებულების შესრულება.

გ) მიმწოდებელი წინამდებარე ხელშეკრულებით გათვალისწინებული პირობების დარღვევისათვის წინამდებარე ხელშკრულების მოქმედების პერიოდში დაჯარიმებულ იქნა სამჯერ.

დ) შემსყიდველისთვის ცნობილი გახდა, რომ მისგან დამოუკიდებელი მიზეზების გამო მიმწოდებელი ვერ უზრუნველყოფს წინამდებარე ხელშეკრულებით ნაკისრი ვალდებულების შესრულებას.
ე) წინამდებარე ხელშეკრულების ვადის გასვლის საფუძველზე.
ვ) ურთიერთშეთანხმების საფუძველზე.
13.2. წინამდებარე ხელშეკრულების ცალკეული პირობების შეწყვეტა არ ათავისუფლებს მიმწოდებელს წინამდებარე ხელშეკრულებით ნაკისრი სხვა ვალდებულების შესრულებისაგან.

14. დავები და მათი გადაწყვეტის წესი

14.1. წინამდებარე ხელშეკრულების შესრულებისას მხარეთა შორის წამოჭრილი დავები ან აზრთა სხვადასხვაობა შესაძლებელია გადაწყვეტილ იქნას ორივე მხარის ერთობლივი მოლაპარაკების საფუძველზე.
14.2. შეთანხმების მიუღწევლობის შემთხვევაში მხარეები მიმართავენ სასამართლოს კანონმდებლობის შესაბამისად.

15. სხვა პირობები

15.1. მხარეები აუნაზღაურებენ ერთმანეთს მიყენებულ ზარალს საქართველოს კანონმდებლობის შესაბამისად.
15.2. არც ერთ მხარეს არა აქვს უფლება გადასცეს მესამე პირს თავისი უფლებები და მოვალეობები, მეორე მხარის წერილობითი თანხმობის გარეშე.
15.3. მესამე პირთან ურთიერთობაში მხარეები მოქმედებენ თავიანთი სახელით, ხარჯებითა და რისკით.
15.4. წინამდებარე ხელშეკრულება შედგენილია ქართულ ენაზე, სამ ეგზემპლარად, რომელთაგან თითოეულს აქვს თანაბარი იურიდიული ძალა და ერთი ეგზემპლარი ინახება მიმწოდებელთან, ორი შემსყიდველთან. წინამდებარე ხელშეკრულებასთან დაკავშირებული ნებისმიერი მიმოწერა შესრულებული უნდა იყოს ქართულ ენაზე.
15.5. წინამდებარე ხელშეკრულების ნებისმიერი ცვლილება ან დამატება ძალაშია მხოლოდ მას შემდეგ, რაც ის იქნება წერილობითი ფორმით შედგენილი და წინამდებარე ხელმოწერილი მხარეთა მიერ.

16. მხარეთა რეკვიზიტები

„შემსყიდველი“	„მიმწოდებელი“
საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტრო მის: ქ. თბილისი, ს. ეულის ქ. N3 ს/კ 204564934 სახელმწიფო ხაზინა კოდი: ს/კ 220101222; ა/ა 200122900 მინისტრის მოადგილე **/ზესიკ დევდარიანი/**	**//**

დანართი N2

პრეტენდენტისშეთავაზება

1.	პრეტენდენტის იურიდიული ფორმა დადასახელება:	
	ხელმძღვანელის თანამდებობა, სახელი და გვარი:	
	პრეტენდენტის იურიდიული ან/და ფაქტიურიმისამართი:	
	საიდენტიფიკაციო კოდი:	
	პრეტენდენტის ტელეფონის ნომერი:	
	ელექტრონული მისამართი:	
	ბანკი:	
	ბანკის კოდი:	
	ანგარიშის ნომერი:	
2.	სახელმწიფო შესყიდვების ერთიან ელექტრონულ სისტემაში შემოთავაზებული სატენდერო წინადადების ფასი:	
3.	ინფორმაცია ანგარიშწორების შესახებ:	
4.	ინფორმაცია საქონლის მიწოდების პირობებისა და ვადების შესახებ:	

პრეტენდენტის ხელმოწერა: _____

ბ.ა.

დანართი N3

ფასების ცხრილი

N	საქონლის დასახელება (ბრენდი და მოდელი)	მწარმოებელი ქვეყანა	ტექნიკური მახასიათებელი	განზ.	რაოდ.	ერთეულის ფასი	საერთო ფასი	მიწოდების ვადა (კალ.დღე)
სულ:								

მიწოდების ადგილი და ფორმა:	
სალიცენზიო გასაღების მოქმდებების ვადა:	

პრეტენდენტის ხელმოწერა: _____

ტექნიკური დავალება

სამუშაო სადგურებისა და სერვერების ანტივირუსული დაცვის პროგრამული საშუალებების გამოყენების უფლება

შესყიდვის სავარაუდო ღირებულება:	**8`000 ლარი (რვაათასი ლარი და 00 თეთრი)**
მომხმარებელთა რაოდენობა:	**300 (სამასი) მომხმარებელი**
მოქმდებების ვადა:	**არანაკლებ 1 წელი**
შესყიდვის ობიექტი:	**ESET NOD32 endpoint Antivirus Business Edition (არსებული ანტივირუსისთვის 1 წლიანი ლიცენზიის განახლება).**

ზოგადი მოთხოვნები

ანტივირუსული დაცვა (ად) უნდა წარმოადგენდეს მასშტაბირებად გადაწყვეტილებას, რომელიც უზრუნველყოფს მყარ ფუნქციონირებას სამუშაო სადგურებისა და სერვერების ლოკალურ ქსელში.

- თავისი ორგანიზაციის ფარგლებში გამოყენებული უნდა იქნას ერთიანი ანტივირუსული საშუალებები, დასამუშავებელი ინფორმაციის კონფიდენციალურობის ხარისხისგან დამოუკიდებლად. ცალკე მდგომი პერსონალური კომპიუტერები, ე.ი. რომლებიც ანტივირუსული დაცვის ერთიან სისტემაზე მიერთებული არ არის, მათ შორის მოშორებულ ტერიტორიაზე მდებარენი, დაცულნი უნდა იქნან ინტეგრირებული საპროგრამო პროდუქტით, რომლებიც შეიცავს დაცვას ზიანისმომტანი პროგრამების ყველა ტიპისაგან. (ანტივირუსი).
- ყველა ანტივირუსული საშუალების პროგრამული ინტერფეისი, მართვის საშუალებების ჩათვლით, უნდა იყოს რუსულ ენაზე.

ანტივირუსული საშუალებები უნდა შეიცავდნენ:

- გასაღების სალიცენზიო ფაილს;
- სამუშაო სადგურებისა და სერვერების ანტივირუსული დაცვის პროგრამულ საშუალებებს;

- ცენტრალიზებული მართვის, მონიტორინგის და განახლებისპროგრამული საშუალებებიOS windows, Linux/BSD/Solaris, Mac OS, მობილურ OS Symbian, windows Mobile, Android-ზე;
- განახლებად მონაცემთა ანტივირუსულ ბაზებს;
- საექსპლუატაციო დოკუმენტაციას რუსულ ენაზე.

მოთხოვნები სამუშაო სადგურების ანტივირუსული დაცვის პროგრამული საშუალებების მიმართ OS მართვით Microsoft Windows-ის ოჯახიდან

სამუშაო სადგურების ანტივირუსული დაცვის პროგრამული საშუალებები Microsoft Windows-ის ოჯახიდან OS მართვით უნდა ფუნქციონირებდნენ OS-ის შემდეგ ვერსიებზე:

- Microsoft Windows 2000 Professional/Server (Service Pack 4 და ზევით);
- Microsoft Windows XP professional;
- Microsoft Windows XP professional x 64 Edition;
- Microsoft Windows Vista;
- Microsoft Windows Vista x 64;
- Microsoft Windows 7;
- Microsoft Windows 7 X 64;
- Microsoft Windows 8;
- Microsoft Windows Server 2003;
- Microsoft Windows Server 2003 x 64;
- Microsoft Windows Server 2003;
- Microsoft Windows Server 2008;
- Microsoft Windows Server 2008 x 64;
- Microsoft WindowsServer 2008 R2;
- Microsoft WindowsServer 2012;

სამუშაო სადგურების ანტივირუსული დაცვის პროგრამული საშუალებები OS Microsoft Windows-ის ოჯახის მართვის ქვეშ უნდა უზრუნველყოფდნენ შემდეგი ფუნქციონალური შესაძლებლობების რეალიზაციას:

- რეზიდენტული ანტივირუსული მონიტორინგი;
- ანტივირუსული სკანირება მომხმარებლის ან ადმინისტრატორის ბრძანებით;
- ანტივირუსული სკანირება განრიგით;
- ანტივირუსული სკანირება მონაცემთა ანტივირუსული ბაზების განახლების შემდეგ;
- ტრაფიკის ანტივირუსული სკანირება შემდეგი ოქმების მიხედვით: FTP, HTTP და HTTPs, POP3 და POR3s, აგრეთვე IMAP და IMAPs ტრაფიკის.
- სკანირების ჩაშვება ზიანის მომტანი კოდის აღმოჩენისას;
- დაცვა ჯერ კიდევ უცნობი ზიანის მომტანი პროგრამებისგან ევრისტიკული ანალიზის საფუძველზე;
- ფარული პროცესების აღმოჩენა;
- ანტივირუსული დაცვის გათიშვის შესაძლებლობა აუცილებლობის შემთხვევაში;
- იმ ფაილების ანტივირუსული შემოწმება და მკურნალობა, რომლებშიც ჩაწყობილია PKLITE, LZEXE, DIET, EXEPACK ტიპის და სხვა პროგრამები;

- ფაილების ანტივირუსული შემოწმება და მკურნალობა ფორმატების ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, YIP, ACE არქივებში;
- Host Intursion Prevention System (HIPS) – შეჭრის თავიდან აცილების დაყენებადობის შემცველობა, გარეგნული ზემოქმედების ცდების თავიდან ასაცილებლად, აგრეთვე პროცესების, ფაილების და რეესტრის გასაღებების მონიტორინგისათვის;
- HIPS მუშაობის შესაძლებლობა ფილტრაციის წინასწარ მომზადებული რეჟიმების რიგით;
- ამოცანების ჩაშვება განრიგის მიხედვით და/ან მყისვე საოპერაციო სისტემის ჩატვირთვის შემდეგ;
- ვებ-რესურსებზე შეღწევით მართვის შესაძლებლობა, დაბლოკილი ანდა ნებადართული ვებ-გვერდების სიის შედგენის გზით;
- ფილტრაციის აქტიური რეჟიმი ჩანრთებისათვის, აგრეთვე გათიშვის შესაძლებლობა;
- ფილტრაციებისანდოჩანართებისათვის;
- სკანირება კონტექსტური მენიუდან;
- ფილტრაციის გათიშვა სანდო ვებ-გვერდებისათვის;
- შემოწმებიდან სანდო პროცესების, ფაილების და პაპკების გამოთიშვის შესაძლებლობა.
- მრავალნაკადიანი სკანირება;
- განახლებების რამოდენიმე პროფილის დაყენება (მაგალითად მობილური მომხმარებლებისთვის) ინტერნეტის ქსელიდან განახლების შესაძლებლობით;
- დამგეგმავის არსებობა კლიენტში;
- ზოგადი ინფორმაციის ნახვის შესაძლებლობა პერსონალური კომპიუტერების მდგომარეობის, დაყენებული ჩანართების, სამსახურების და ა.,შ. შესახებ, ცვლილებების დაკვირვების და მათი სურათების დახმარებით შედარებების შესაძლებლობით;
- პერსონალური კომპიუტერის გადატვირთვის აუცილებლობის არარსებობა, ანტივირუსული პროგრამული უზრუნველყოფის (აპუ) დაყენების შემდეგ, კლიენტის სამუშაო სადგურზე;
- სამუშაო სადურების ანტივირუსული დაცვის უკვე დაყენებული ლიცენზიების მიერთების შესაძლებლობა ცენტრალური მართვის კონსოლისადმი, დამატებითი PO-ს
- დაყენების აუცილებლობის გარეშე;
- მონაცემთა ანტივირუსული ბაზის გაშვება მოდემური შეერთების ან VPN-ის დაყენების შემდეგ;
- სხვა მწარმოებლის ჩანართის გაშვების ამოცანის შექმნის შესაძლებლობა ანტივირუსის დაგეგმვაში;
- ზიანის მომტანი სცენარებისგან დაცვა, რომლებიც იტვირთება ვებ-გვერდებიდან და ფიშინგ-საიტების გამოცნობა;
- საფოსტო კლიენტების დაცვა: Microsoft Outlook, Outlo OS Express,Windows mail, Windovs Live Mail, Moyilla Thunderbird;
- სკანირების პროცესების დაჩქარება, იმ ობიექტების გაშვების ხარჯზე, რომელთა მდგომარეობაც წინა შემოწმების დროიდან არ შეცვლილა;
- სამუშაო სადგურის რესურსების განაწილების რეგულირება ანტივირუსსა და სხვა ჩანართებს შორის ამოცანების პრიორიტეტულობაზე დამოკიდებულებით: ანტივირუსული სკანირების ფონურ რეჟიმში გაგრძელების შესაძლებლობა;
- სკანირების ლიმიტების მომართვა პარამეტრების მიხედვით – ჩადებების (არქივების) სიღრმე, ობიექტის და ობიექტის სკანირების დროის სიდიდეები;
- იმ მოდულის არსებობა, რომელიც საშუალებას იძლევა ჩატარებული იქნას მონაცემების შენახვის მიერთებადი გარე მოწყობილობების შინაარსის ავტომატური სკანირება, აგრეთვე გამოყენებული იქნას გაფართოებული ანალიზი ასეთი მოწყობილობებიდან ფაილის ჩასაშვებად;
- იმ მოდულის არსებობა, რომელიც საშუალებას იძლევა აწყობილი იქნას მიღწევადობის შეზღუდვები (არ არის მიღწევადობა, მხოლოდ კითხვა, სრული მიღწევადობა) თითოეული მომხმარებლისთვის ან მომხმარებელთა ჯგუფისათვის, როგორც მოწყობილობის ტიპის (CD/DVD/Blu-Ray, USB მონაცემების საცავი, USB პრინტერ, გამოსახულების დამუშავების მოწყობილობები, მოწყობილობა Fire Wire, რიდერების, მოდემების კადრი, LPT/COM პორტები, Bluetooth მოწყობილობები), ასევე უკანა ატრიბუტების მიხედვით.
- ინტეგრაცია MS NAP-დან;
- მეხსიერების ავარიული დამპების ფორმირების შესაძლებლობა, დამატების ჩამოგდების შემთხვევაში
- კლიენტის ყველა მოდულის სრულფუნქციონირებადი შრომისუნარიანობის შესაძლებლობა, სალიცენზიო ფაილის გარეშე;

- სავირუსო ბაზების განახლებების გადახვევის შესაძლებლობა წინა ვერსიებზე და მათი განახლებების გაჩერება განახლების შემდგომი ავტომატური ჩართვით, დროის ხსენებულ შუალედში;
- ინტეგრაცია Windows ინტეგრაციის ცენტრთან;
- ინტეგრაცია Windows განახლების ცენტრთან;
- კომპიუტერის შესრულებადი ფაილების და დასატვირთი სფეროების შემოწმების მომართვა, ცალკე ამოცანის სახით;
- ანტივირუსული პროდუქტების თვითდაცვა ზიანის მომტანი პროგრამებისგან, ბოროტ განმზრახველებისგან ან არაკვალიფიცირებული მომხმარებლებისგან;
- სისტემის აქტუალური განახლებების არსებობის შემოწმება;
- უწყებების ავტომატური დამალვა ანტივირუსის მუშაობისას სრული ეკრანის რეჟიმში;
- სამუშაო სადგურებზე მომხდარი მნიშვნელოვანი მოვლენების შესახებ ადმინისტრატორისათვის შეტყობინების მრავალი გზის არსებობა (საფოსტო შეტყობინება, ამოცურებადი ფანჯარა, ჩანაწერი მოვლენების ჟურნალში);
- პროგრამული საშუალებების და ანტივირუსული ბაზების განახლება სხვადასხვა წყაროებიდან, როგორც კავშირგაბმულობის არხებით, ასევე ინფორმაციის გასასხვისებელ მატარებლებზე;
- ლოგოების ექსპორტი ფორმატებში XML, TXT, DAT;
- უცნობი საფრთხეების დეტექტირების ტექნოლოგიის არსებობა, დამატებების კონტროლი რეპოუტაციული სერვისის საფუძველზე;
- ზიანის მომტანი კოდის ვირუსული ექსპერტებისადმი გადაცემის სისტემის არსებობა ავტომატურად ან ხელით;
- ავარიული აღმდგენის დისკების შექმნის შესაძლებლობა;
- ელექტროენერგიის ეკონომია ავტონომიური კვების რეჟიმში;
- სისტემური მოთხოვნები სამუშაო სადგურის მიმართ – 128 Mb RAM, HDD 320 Mb, 400 MG c Processor 32-bit 9x86) და 64-bit 9x64) Intel. AMD ან 100% შეთავსებადები;
- ანტივირუსის დისტრიბუტივის სიდიდე არ უნდა აჭარბებდეს - 80 Mb-ს.

მოთხოვნები სამუშაო სადგურების ანტივირუსული დაცვის პროგრამული საშუალებების მიმართ OS მართვით Microsoft Windows-ის ოჯახიდან

სერვერების სისტემების ანტივირუსული დაცვის პროგრამული საშუალებები Microsoft Windows-ის ოჯახიდან OS მართვით უნდა ფუნქციონირებდნენ OS-ის შემდეგ ვერსიებზე:

- Microsoft Windows 2000 Server/Advanced Server (Service Pack 4 და ზევით, ყველა მიმდინარე განახლება);
- Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windovs Server 2003 web Edition, Microsoft windows storage4 server 2003, Microsoft Small Business Server 2003 ყველა Service Packs 4 ყველა მიმდინარე განახლება);
- Microsoft Windows Server 2003 R2 Standard x 64 Edition,Microsoft Windovs Server 2003 R2 Enterprise x 64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft windows Server 2003 R2 enterprise Edition;
- Microsoft Windows Server 2008 Standard,Microsoft Windovs Server 2008 Datacenter, Microsoft Windows Server 2008 R2 Enterprise, Microsoft windows Server 2008 Standard,Microsoft Windows Server 2008 .
- Microsoft Windows Server 2008 R2 Standard Edition,Microsoft Windows Server 2008 R2 Enterprise Edition, Microsoft Windows Server 2008 R2Datacenter Edition, Microsoft windows Server 2008 R2 Foundation Edition;
- Microsoft Windows Small Business Server 2008
- Microsoft Windows Small Business Server 2011

- Microsoft Windows Server Core 2008
- Microsoft Windows Server Core 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server Core 2012

ფაილის სერვერების ანტივირუსული დაცვის პროგრამული საშუალებები OS Microsoft Windows-ის ოჯახის მართვის ქვეშ უნდა უზრუნველყოფდნენ შემდეგი ფუნქციონალური შესაძლებლობების რეალიზაციას:

- რეზიდენტული ანტივირუსული მონიტორინგი;
- ანტივირუსული სკანირება მომხმარებლის ან ადმინისტრატორის ბრძანებით;
- ანტივირუსული სკანირება განრიგით;
- ანტივირუსული სკანირება მონაცემთა ანტივირუსული ბაზების განახლების შემდეგ;
- ტრაფიკის ანტივირუსული სკანირება შემდეგი ოქმების მიხედვით: FTP, HTTP და HTTPs, აგრეთვე POP3 და POR3s, ტრაფიკის.
- სკანირების ჩაშვება ზიანის მომტანი კოდის აღმოჩენისას;
- დაცვა ჯერ კიდევ უცნობი ზიანის მომტანი პროგრამებისგან ევრისტიკული ანალიზის საფუძველზე;
- რუტიკების (მალული ფაილების/სისტემური ანომალიების) აღმოჩენა;
- იმ ფაილების ანტივირუსული შემოწმება და მკურნალობა, რომლებშიც ჩაწყობილია PKLITE, LZEXE, DIET, EXEPACKტიპის და სხვა პროგრამები;
- ფაილების ანტივირუსული შემოწმება და მკურნალობა ფორმატების ARJ,BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, YIP, ACE არქივებში;
- ამოცანების ჩაშვება განრიგის მიხედვით და/ან მყისვე საოპერაციო სისტემის ჩატვირთვის შემდეგ;
- სხვა მწარმოებლის ჩანამატის გაშვების ამოცანის შექმნის შესაძლებლობა ანტივირუსის დამგეგმავში;
- ზიანის მომტანი სცენარებისგან დაცვა, რომლებიც იტვირთება ვებ-გვერდებიდან და ფიშინგ-საიტების გამოცნობა;
- სერვერზე ფაილების ავტომატური აღმოჩენისა და გამორიცხვის ფუნქცია, რომელთაც კრიტიკული მნიშვნელობა აქვთ უწყვეტი მუსაობისათვის;
- კანირების მოდულების რაოდენობის მიცემის შესაძლებლობა, სკანირების სისწრაფის გასაზრდელად;
- ვებ-რესურსბზე შეღწევით მართვის შესაძლებლობა, დაბლოკილი ანდა ნებადართული ვებ-გვერდების სიის შედგენის გზით;
- ფილტრაციის აქტიური რეჟიმი ჩანრთებისათვის, აგრეთვე გათიშვის შესაძლებლობა;
- ფილტრაციებისანდოჩანართებისათვის;
- სკანირება კონტექსტური მენიუდან;
- ფილტრაციის გათიშვა სანდო ვებ-მისამართებისათვის;
- მრავალნაკადიანი სკანირება;
- განახლებების რამოდფენიმე პროფილის დაყენება (მაგალითად მობილური მომხმარებლებისთვის) ინტერნეტიდან განახლების შესაძლებლობით;
- დამგეგმავის არსებობა კლიენტში;
- ზოგადი ინფორმაციის ნახვის შესაძლებლობა პერსონალური კომპიუტერების მდგომარეობის, დაყენებული ჩანართების, სამსახურების და ა.,შ. შესახებ, ცვლილებების დაკვირვების და მათი სურათების დახმარებით შედარებების შესაძლებლობით;
- ანტივირუსული პაკეტის პარამეტრების მომართვის შესაძლებლობა ბრძანებითი ბწკარის ინტერფეისიდან;
- უცნობი საფრთხეების დეტექტირების ტექნოლოგიის არსებობა,
- პერსონალური კომპიუტერის გადატვირთვის აუცილებლობის არარსებობა, ანტივირუსული პროგრამული უზრუნველყოფის (აპუ) დაყენების შემდეგ;
- სამუშაო სადგურების ანტივირუსული დაცვის უკვე დაყენებული ლიცენზიების მიერთების შესაძლებლობა ცენტრალიზებული მართვის კონსოლისადმი, დამატებითი PO-სადენების აუცილებლობის გარეშე;

- მონაცემთა ანტივირუსული ბაზის გაშვება მოდემური შეერთების ან VPN-ის დაყენების შემდეგ;
- სკანირების პროცესების დაჩქარება, იმ ობიექტების გაშვების ხარჯზე, რომელთა მდგომარეობაც წინა შემოწმების დროიდან არ შეცვლილა;
- სამუშაო სადგურის რესურსების განაწილების რეგულირება ანტივირუსსა და სხვა ჩანართებს შორის ამოცანების პრიორიტეტულობაზე დამოკიდებულებით: ანტივირუსული სკანირების ფონურ რეჟიმში გაგრძელების შესაძლებლობა;
- სკანირების ლიმიტების მომართვა პარამეტრების მიხედვით – ჩადებების (არქივების) სიღრმე, ობიექტის და ობიექტის სკანირების დროის სიდიდეები;
- ინფორმაციებისა და მოწყობილობების ცვლადი მატარებლების ბლოკირება (USB)
- ინტეგრაციაWindows –ის უსაფრთხოების ცენტრთან;
- ინტეგრაციაWindows განახლების ცენტრთან;
- კომპიუტერის შესრულებადი ფაილების და დასატვირთი სფეროების შემოწმების მომართვა, ცალკე ამოცანის სახით;
- ანტივირუსული პროდუქტების თვითდაცვა ზიანის მომტანი პროგრამებისგან, ბოროტგანმზრახველებისგან ან არაკვალიფიცირებული მომხმარებლებისგან;
- საოპერაციო სისტემის აქტუალური განახლებების არსებობის შემოწმება;
- სრულყოფილი მუშაობა გრაფიკული ინტერფეისის გარეშე აპუ-ს ადმინისტრირება და კონფიგურირება, ბრძანებითი ბწკარით.
- სამუშაოს ავტომატიზაციის შესაძლებლობა იმ სცენარების შესრულების ხარჯზე, რომლებიც აპუ-ს კონფიგურირების და რაიმე ქმედების შესრულების შესაძლებლობას იძლეოდა;
- შეტყობინებების ავტომატური გახსნა ანტივირუსის მუშაობისას ნახევარეკრანულ რეჟიმში;
- სერვერებზე მომხდარი მნიშვნელოვანი მოვლენების შესახებ ადმინისტრატორისათვის შეტყობინების მრავალი გზის არსებობა (საფოსტო შეტყობინება, ამოცურებადი ფანჯარა, ჩანაწერი მოვლენების ჟურნალში);
- პროგრამული საშუალებების და ანტივირუსული ბაზების განახლება სხვადასხვა წყაროებიდან, როგორც კავშირგაბმულობის არხებით, ასევე ინფორმაციის გასასხვისებელ მატარებლებზე;
- ზიანის მატარებელი კოდის ნიმუსების ვირუსულ ექსპერტებზე გადაცემის სისტემის არსებობა ავტომატურად ან ხელით;
- ავარიული აღდგენის დისკების შექმნის შესაძლებლობა
- სისტემური მოთხოვნები სამუშაო სადგურის მიმართ – 128 Mb RAM, HDD 320 Mb, 400 MG c Processor 32-bit 9x86) და 64-bit 9x64) Intel, AMD ან 100% შეთავსებადები;
- ანტივირუსის დისტრიბუტივის ზომა 60 Mb-ს არ უნდა აჭარბებდეს.

მოთხოვნებიმობილური მოწყობილობების ანტივირუსული დაცვის საშუალებების მიმართ

პროგრამული საშუალებები სმარტფონების ანტივირუსული დაცვისთვის უნდა ფუნქციონირებდეს მობილური OS –ის მართვის ქვეშ:

- Symbian S60 3rd Edition Feature pack 1 ან 2 (მხოლოდ Nokia)
- Symbian S60 5th Edition (Nokia only)
- Symbian 3 (Nokiaonly)
- Windows mobile 5.0, 6.0, 6.1 და 6.5
- Android 2.0 და ზევით

სმარტფონების ანტივირუსული დაცვის პროგრამულმა საშუალებებმა უნდა უზრუნველყონ შემდეგი ფუნქციონალობა:

- მოწყობილობის უსაფრთხოების აუდიტის ჩატარების შესაძლებლობა ანგარიშის გენერაციით;
- სმარტფონის ფაილური სისტემის მუდმივი დაცვა;
- ყველა დანამატის, ფაილების, პაპკების და მეხსიერების ბარათის შემოწმება რეალური დროიწს რეჟიმში;
- სმარტფონზე ან მეხსიერების გაფართოების მიერთებულ ბარათებზე არსებული ფაილური სისტემის ობიექტების შემოწმება, მომხმარებლის მოთხოვნით და განრიგის მიხედვით;
- დასნებოვნებული ობიექტების საიმედო იზოლირება კარანტინულ შემნახველში;
- იმ ანტივირუსული ბაზების განახლება, რომლებიც გამოიყენება ზიანის მომტანი პროგრამების ზებნისას და სახიფათო ობიექტების მოცილებისას;
- არასასურველიSMS და MMS შეტყობინებების ბლოკირება;
- დაცვა სმარტფონის მოპარვისა და დაკარგვისაგან. მობილური მოწყობილობის მოცილებული ბლოკირების შესაძლებლობის უზრუნველყოფა;
- სმარტფონიდან ინფორმაციის დისტანციურად მოცილების უზრუნველყოფა;
- სანდო SIM-ბარათის განსაზღვრის შესაძლებლობა;
- უწყების ავტომატური ფარული გაგზავნა SMS შეტყობინების საშუალებით, გაფრთხილებით არასანდო SIM-ბარათის გამოყენების შესახებ. შეტყობინება უნდა შეიცავდეს აგრეთვე ბოროტგანმზრახველის იდენტიფიკაციისატვის აუცილებელ ინფორმაციას: მიმდინარე SIM-ბარათის ტელეფონის ნომერს, IMSI-ის ნომერს და IMEI;
- სისტემური მოთხოვნები: OS Windows Mobile 5.0 ან უფრო გვიანი ვერსიისთვის – ასეთია პროცესორის 200 MGc სიხშირე, მეხსიერების მოცულობა 16 MB, დისკზე თავისუფალი ადგილის მოცულობა 2,5MB. OS S60 3rd Edition Feature Pack 1 თვის ან 2 (Nokia) S60 5th Edition (Nokia) Symbian 3 (Nokia)-თვის- თავისუფალი ადგილის მოცულობა დისკზე 2 MB.
- სისტემური მოთხოვნები: Android 2.0–თვის და ზევით - 600MGc პროცესორის ტაქტური სიხშირე, მეხსიერების მოცულობა 256 MB, თავისუფალი ადგილის მოცულობადისკზე 5 MB.

მოთხოვნები ანტივირუსული დაცვის მართვის სისტემის მიმართ

მართვის პროგრამული სისტემები ყველა დამცავი რესურსისათვის უნდა უზრუნველყოფდნენ შემდეგი ფუნქციონალური შესაძლებლობების რეალიზაციას:

- მასშტაბული გადაწყვეტილება;
- ცენტრალიზებული დანადგარი/განახლება/ანტივირუსული დაცვის პროგრამული საშუალებების, მომართვის, ადმინისტრირების მოცილება;
- ინფორმაციის ცენტრალიზებული შეკრება და მოხსენების შექმნა ანტივირუსული დაცვის მდგომარეობის შესახებ;
- დაცული შეერთება სერვერსა და კლიენტს შორის;
- WEB-კონსოლის არსებობა;
- მოხსენებების შექმნა თვალისჩინო გრაფიკული სახით;
- SIEMმხარდაჭერის მოდულის არსებობა;
- კლიენტების წინასწარი განწყობა და კონფიგურაციის ფაილების შენახვის შესაძლებლობა შემდგომი გამოყენებისათვის (განახლებების პროფილები, აკრძალული საიტები, დამგეგმავის განრიგი და ა.შ.);
- სამომხმარებლო დანამატების დაყენების შესაძლებლობა;
- კლიენტის ნაწილის დაყენების შესაძლებლობა ე-მაილით;
- მოშორებული დანადგარის წინასწარი დიაგნოსტიკის შესაძლებლობა;

- მოშორებული დანადგარი შესვლის სცენარის დახმარებით;
- უსაფრთხოების პოლიტიკის დაყენება კლიენტებისათვის;
- პერს. კომპიუტერის მდგომარეობის შესახებ, დაყენებული დამატებების და ა.შ. ზოგადი ინფორმაციის ნახვის შესაძლებლობა, ცვლილებებზე დაკვირვების და მათი შედარების შესაძლებლობით, სურათების დახმარებით.
- დამატებითი PO-ს დაყენების აუცილებლობის არარსებობა სერვერის და ადმინისტრირების კონსოლის დასაყენებლად
- იერარქიის შექმნა მთავარი და დაქვემდებარებული სერვერებისგან. რეპლიკაცია მათ შორის, ყველა კლიენტის მართვის შესაძლებლობით Mმთავარი სერვერიდან;
- პერს.კომპიუტერის გადატვირთვის აუცილებლობის არარსებობა APO-ს კლიენტის დაყენების შემდეგ.
- ანტივირუსული დაცვის და ანტივირუსული ბაზების პროგრამული საშუალებების ავტომატიზირებული განახლება;
- სიგნატურული ბაზების გადახვევის შესაძლებლობა;
- განახლებების მიტანა მომხმარებელთა სამუშაო ადგილას, მყისვე მათი მიღებიდან;
- ცენტრალიზებული კარანტინი;
- კომპიუტერთა ჯგუფის ავტომატური შექმნის შესაძლებლობა AD-თან სინქრონიზაციის გზითY;
- AD-თან სინქრონიზაციის შესაძლებლობა, როგორც განრიგით, ასევე ხელით;
- დაუცველი სამუშაო სადგურების ავტომატური ძებნა, ქსელის ტოპოლოგიის გათვალისწინებით;
- ცვლილებების აუდიტი სერვერების მომართვებში სააღრიცხვო ჩანაწერების მიხედვით;
- მოშორებული დანადგარის შესაძლებლობები ოპერაციულ სისტემებზე Windows, linux, MacOSოჯახიდან;
- დაცვის თვისებების ცვლილების შესაძლებლობა, მოახდინოს მოდული დეაქტივირება დროის განსაზღვრულ ინტერვალზე;
- მართვის მრავალდონიანი სისტემის აგება ადმინისტრატორებისა და ოპერატორების როლების, აგრეთვე წარმოსადგენი ანგარიშგების ფორმების მომართვის შესაძლებლობით,თითოეულ დონეზე;
- პროგრამული საშუალებების და ანტივირუსული ბაზების განახლება სხვადასხვა წყაროებიდან, როგორც კავშირგაბმულობის არხებით, ასევე ინფორმაციის მატარებლებით;
- ანტივირუსული დაცვის დაყენებული დამატებების (ჩანართების) მუშაობაში მოვლენების შესახებ შეტყობინების მექანიზმი და მათ შესახებ საფოსტო უწყებების დაგზავნის აწყობის შესაძლებლობა;
- ზიანის მომტანი კოდის ვირუსულ ექსპერტებზე გადაცემის სისტემის არსებობა ავტომატურად და ხელით;
- ჯგუფის შექმნის შესაძლებლობა, რომელშიც დინამიკურად იქნება ჩართული კლიენტის სადგურები მოცემული ჯგუფის პირობების შესაბამისობისას;
- დამატებითი მოდულების (კლიენტების/აგენტების) არარსებობა პერს. კომპ. მოშორებულ სერვერზე შორეული ადმინისტრირების უზრუნველსაყოფად;
- ქსელის ადმინისტრატორის უწყებების სხვადასხვა ვარიანტები (ჩანაწერი ფაილში, სისტემურ ლოგში, ე/მაილით, SNMP- ხაფანგები, ჩაშვება რომელიმე ფაილის შესასრულებლად;
- მონაცემთა ბაზის შემცველობის სარეზერვო ასლების შექმნის და სერვერის დაყენების შესაძლებლობა;
- კონსოლის შორეული ადმინისტრირების სერვერისადმი მიერთების შესაძლებლობა მომხმარებლის სახელის და პაროლის გამოყენებით;
- Windows,Linux/BSD/Sun- სერვერების და სამუშაო სადგურების, აგრეთვე მობილური OS (Symbian და Microsoft Windows Mobile) დაცვის გადაწყვეტილებების ადმინისტრირება;
- Access, MS SOL,Oracle, MySQL- მონაცემთა ბაზის მხარდაჭერა;
- შორეული ადმინისტრირების სერვერმა მხარი უნდა დაუჭიროს საოპერაციო სისტემებს XP, Vista,7,8 და Windows Server 2000, 2003, 2008, 2012, Ubuntu, RedHat, CentOS, OpenSUSE, Debian, Fedora;
- შორეული ადმინისტრირების სერვერის დისტრიბუტისვის სიდიდე – არა უმეტეს 70 Mb;
- შორეული ადმინისტრირების კონსოლის დისტრიბუტისვის სიდიდე – არა უმეტეს 17 Mb;

- სისტემური მოთხოვნები ადმინისტრირების სერვერის და კონსოლის მიმართ დისტრიბუტისვის– არა უმეტეს 256 Mb RAM, HDD 100 Mb, 300 MGc Processor 32-bit (x86) და 64-bit (x64) intel, AMD ან 100% შეთავსებადები;

მოთხოვნები ანტივირუსული ბაზების განახლების მიმართ

განახლებადი მონაცემთა ანტივირუსული ბაზები უნდა უზრუნველყოფდნენ შემდეგი ფუნქციონალური შესაძლებლობების რეალიზაციას;

- რეალიზებულია განახლებების სარკის შექმნის შესაძლებლობა ტარიფის ეკონომიისათვის;
- განახლებების სარკე შესაძლებელია შექმნას ნებისმიერი პერს. კომპ. ქსელზე
- განახლებების ტიპები: ვირუსების BD სიგნატურების, პროგრამული კომპონენტების განახლება, ბირთვის განახლება;
- სარკის განახლების პაკეტები შეძლება დატვირთული იქნას ორი მეთოდით: NTTP ოქმის მიხედვით (რეკომენდირებულია) და საერთო ქსელური დისკის (SMB) დახმარებით;
- განახლებანი შეიძლება გავრცელებული იქნას ინფორმაციის ელექტრონულ მატარებლებზე (FDD/CD/DVD/USB-drive);
- ხორციელდება განახლებების მთლიანობისა და ნამდვილობის შემოწმება ელექტრონული ციფრული ხელმოწერის საშუალებებით.

მოთხოვნები საექსპლუატაციო დოკუმენტაციის მიმართ

საექსპლუატაციო დოკუმენტაცია ყველა ანტივირუსული დაცვის პროგრამული პროდუქტისათვის, მართვის საშუალებების ჩათვლით, უნდა შეიცავდეს დოკუმენტებს რუსულ ენაზე, მათ შორის:

- მომხმარებლის (ადმინისტრატორის) სახელმძღვანელოს;
- შორეული ადმინისტრირების საშუალებების ადმინისტრატორის სახელმძღვანელოს.
- დოკუმენტაცია, რომელიც ანტივირუსული საშუალებებით მოეწოდება, დეტალურად უნდა აღწერდეს ანტივირუსული დაცვის შესაბამისი საშუალების დაყენების, მომართვის და ექსპლუატაციის პროცესს.

მოთხოვნები ტექნიკური მხარდაჭერის მიმართ

ანტივირუსული პროგრამული უზრუნველყოფის ტექნიკური მხარდაჭერა:

- წარმოდგენილი უნდა იყოს რუსულ ენაზე ანტივირუსული დაცვის მწარმოებლის სერტიფიცირებული სპეციალისტის მიერ, რუსეთის ფედერაციის მთელ ტერიტორიაზე დღე-ღამის განმავლობაში, დღესასწაულებისა და გამოსასვლელი დღეების გარეშე (24x7) ელექტრონულ ფოსტაზე და ინტერნეტით;
- ანტივირუსული დაცვის Web-საიტი უნდა იყოს რუსულ ენაზე, ჰქონდეს სპეციალური განყოფილება, რომელიც მიძღვნილი იქნება ტექნიკური მხარდაჭერისადმი, რომელიც ავსებს ცოდნის ბაზას და რუსულენოვან ფორუმს.