3. შესყიდვის ობიექტის მიწოდების ვადა და ტექნიკური დავალება:

- მიმწოდებელმა უნდა უზრუნველყოს შესყიდვის ობიექტის მიწოდება ხელშეკრულების გაფორმებიდან 7 (შვიდი) კალენდარულ დღეში.
- მოწოდებული პროგრამული პაკეტების ლიცენზიების მოქმედების ვადა უნდა იყოს 1 (ერთი) წელი;
- **შესყიდვის ობიექტია:** ანტივირუსული პროგრამული პაკეტის 1 (ერთი) წლიანი ლიცენზია **900** მომხმარებელზე/მოწყობილობაზე (სერვერული სისტემისათვის და საოფისე კომპიუტერისათვის), ანტივირუსული/ანტისპამ დაცვა Microsoft Exchange სერვერსითვის 1800 ელ-ფოსტის მეილბოქსზე, 1 ცალი კრიპტოგრაფიული უსაფრთხოების SSL სერტიფიკატი და სენდბოქს სერვისი/ლიცენზია **700** მომხმარებელზე.

შენიშვნა: - შემსყიდველს ამ ეტაპზე შემენილი აქვს ანტივირუსული პროგრამული პაკეტის 1 (ერთი) წლიანი ლიცენზია 800 მომხმარებელზე/მოწყობილობაზე (სერვერული სისტემისათვის და საოფისე კომპიუტერისათვის), ანტივირუსული/ანტისპამ დაცვა Microsoft Exchange სერვერსითვის 900 ელ-ფოსტის მეილბოქსზე, 1 ცალი კრიპტოგრაფიული უსაფრთხოების SSL სერტიფიკატი და სენდბოქს სერვისი/ლიცენზია 400 მომხმარებელზე. (იხ.**SPA200001310**) რომლის მოქმედების ვადა იწურება 2021 წლის 16 აპრილს), იმ შემთხვევაში თუ პრეტენდენტის მიერ შემოთავაზებული იქნება ანალოგიური ანტივირუსული პროგრამული პაკეტი, მაშინ შესაძლებელია შესაბამის რაოდენობებზე შემოთავაზებული იქნას აღნიშნული ანტივირუსული პაკეტის განახლება (გაგრძელება);

ანტივირუსული პროგრამა უნდა უზრუნველყოფდეს:
სერვერული და საოფისე სისტემებისათვის

•თავსებადობა Microsoft Windows-ის კომპიუტერულ ოპერაციულ სისტემებთან: Windows 10, 8.1, 8, 7

•თავსებადობა Microsoft Windows-ის სერვერულ ოპერაციულ სისტემებთან: Windows Server 2019, 2016, 2012, 2012 R2, 2008, და Linux (Suse, Ubuntu, Debian, RedHat, CentOS) სისტემებთან

• თავსებადობა სმარტფონების და პლანშეტების ანტივირუსული დაცვისთვის Android 5 და ზევით.

• ანტივირუსული დაცვა ყველა ტიპის ვირუსული საშიშროებისგან viruses, rootkits, worms spyware, trojan

• პროაქტიული დაცვას, რაც გულისხმობს ისეთი ვირუსების გამოვლენას, რომელთა შესახებ პროგრამის ბაზაში ინფორმაცია არ მოიძებნება.

• შეიცავდეს Host Based Intrusion Prevention System (HIPS)-ის გარეგანი ზემოქმედების მცდელობის ასარიდებლად და ასევე პროცესების, რეგისტრების და ფაილების მონიტორინგისთვის. საშიშროებების აღმოჩენა სისტემის ქცევის ანალიზის მიხედვით.

• უცნობი საშიშროებისგან დაცვა ევრისტიკული ანალიზის საფუძველზე.

•Microsoft office დოკუმენტების დაცვის დამატებითი მოდულის არსებობა. დოკუმენტების შემოწმება მათ გახსნამდე.

• შიფრატორებისგან დაცვა (Ransomware Shield)

- Exploit-ების ბლოკირება - სხვადასხვა აპლიკაციებში (ბრაუზერები, დოკუმენტის წამკითხავი, flash, Java და სხვა) ქცევის ანალიზი და მონიტროინგი საეჭვო და მავნე აქტივობებზე.
- დაცვა ბოტნეტებისგან - მავნე პროგრამების/ვირუსების აღმოჩენა მათი მონაცემთა მიმოცვლის სქემის და პროტოკოლების ანალიზის საშუალებით.
- პროცესების ანალიზის, ქცევის შესაბამისად საეჭვო აქტიურობის გამოვლენა/ბლოკირება.

- ფაილებსა და სისტემის რეგისტრებზე აპლიკაციებისა და პროცესების აკრძალვის/დაშვების შესაძლებლობა.
- UEFI-ის სკანირების შესაძლებლობა

• შემდეგი არქივირებული ფაილების ტიპების შემოწმება და განკურნვა: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE;

- რუტკიტების (დაფარული ფაილების/სისტემური ანომალიების) აღმოჩენა.
- ტრაფიკის ანტივირუსული სკანირება შემდეგი პროტოკოლებით : FTP, HTTP, HTTPs, POP3
- სანდო პროცესების, ჰეშ-ჯამების, ფაილების და საქაღალდეების შემოწმების გამორიცხვა
- მეხსიერების სკანირების მოდულის არსებობას, რომელიც აკონტროლებს პროცესების ქცევას და ასკანერებს საზიანო პროცესებს როცა ისინი იხსნიან შენიღბვას მეხსიერებაში.

• გარე წამკითხავი USB, DVD, CD და სხვა მოწყობილობების (მათ შორის მობილური კავშირგაბმულობის საშუალებები) ავტომატური სკანირება შეერთებისას.

- მოწყობილობების კონტროლი - ინფრომაციის შეცვლადი მატარებლებისა და მოწყობილობების ბლოკირება, ცალკეული ჯგუფისა ან მომხმარებლისათვის მოწყობილობათა ტიპის (CD/DVD/Blu-Ray, USB, FireWire, Card-Reader, Modem, LPT\COM ports, Bluetooth) მიხედვით, მათ შორის მოწყობილობის სერიული ნომრის, მოწყობილობის ტიპის და მწარმოებლის მიხედვით.

• დაცვას ინტერნეტ საფრთხეებისაგან, ვებ გვერდების შემოწმება/ბლოკირება მავნე კოდებსა, ზიანის მომტანი ლინკებისგან, Web-გვერდებიდან ატვირთული საზიანო სცენარებისგან დაცვა და საეჭვო ფიშინგ გვერდის ბლოკირება - Anti-Phishing მოდულის არსებობა, ვებ-რესურსებისადმი წვდომის მართვის შესაძლებლობა, დაბლოკილი ან ნებადართული ვებ-გვერდების სიის შექმნა.

- ელ-ფოსტის პროგრამებში ინტეგრაცია და ელ-ფოსტის სკანირება: Microsoft Outlook
- ინტეგრაცია Windows-ის განახლების ცენტრთან (სისტემის აქტუალური და კრიტიკული განახლებების არსებობის შემოწმება და მათი ამორჩევითი ინსტალაცია).
- ინტეგრაცია Windows-ის უსაფრთხოების ცენტრთან.
- ინტეგრაცია MS NAP -თან (Network Access Protection).
- კლიენტში განრიგების ორგანიზატორის არსებობა.
- სკანირების პროცესის აჩქარება იმ ობიექტების გამოტოვების ხარჯზე, რომელთა მდგომარეობა წინა შემოწმების შემდეგ არ შეცვლილა.
- სკანირების სიღრმის დარეგულირება პარამეტრების მიხედვით, არქივების, ობიექტის ზომის.
- უცნობი საშიშროების აღმოჩენის ღრუბლოვანი ტექნოლოგიის არსებობა, კონტროლი რეპუტაციის სერვისის მიხედვით.
- ლოგ ფაილების ექსპორტირება XML,TXT ფორმატებში.
- საჭიროების შემთხვევაში ანტივირუსული დაცვის გამორთვის შესაძლებლობა
- ავარიული აღდგენის დისკის შექმნის შესაძლებლობა.
- მომხმარებელთა ანტივირუსული ბაზის ავტომატური განახლების საშუალება, როგორც შიდა ქსელის ადმინისტრირების სერვერის, ასევე ინტერნეტის საშუალებით;
- სამუშაო სადგურის ანტივირუსსა და სხვა აპლიკაციებს შორის რესურსების განაწილების რეგულირებას ამოცანების პრიორიტეტულო ბის მიხედვით: ფონურ რეჟიმში ანტივირუსული სკანირების გაგრძელების შესაძლებლობა.
- მომხმარებელთა ანტივირუსული ბაზის ავტომატური განახლების საშუალება, როგორც შიდა ქსელის ადმინისტრირების სერვერის, ასევე ინტერნეტის საშუალებით;
- საჭიროებისამებრ ვირუსის საზიანო კოდის ავტომატურად ან ხელით გადაცემის შესაძლებლობა მწარმოებლის სპეციალისტებისთვის ანალიზისთვის.

- სერვერ - კლიენტის ცენტრალიზებული ინსტალაციის და მართვის შესაძლებლობა, WEB-კონსოლის არსებობა;
- კომპიუტერის მდგომარების შესახებ, მასში დაყენებული აპლიკაციების, სერვისების , ქსელური შეერთებების შესახებ ინფორმაციის ცენტრალიზებული ნახვის შესაძლებლობა.
- საჭიროებისამებრ ჩაშენებული სენდბოქს სისტემის მხარდაჭერა (საეჭვო და საფრთხის შემცველი ფაილების ემულაცია, რომელიც სხვადასხვა მეთოდის გამოყენებით ახდენს საფრთხეების აღმოჩენას)
- მოქნილი ადმინისტრირება - ლიცენზიის ადმინისტრირების და ლიცენზირებული მომხმარებლების შემოწმების საშუალება ვებ ბრაუზერით.
- ანტივირუსული პროგრამული უზრუნველყოფის ერთი სალიცენზიო ფაილი(გასაღები) 900 მომხმარებელზე (სამუშაო კომპიუტერებისათვის და სერვერებისათვის), ასევე მომხმარებლის სახელი, პაროლი და სერიული ნომერი.

მოთხოვნები ანტივირუსული დაცვის, ცენტრალიზებული მართვის სისტემისადმი:

- ანტივირუსული დაცვის, რეგულირების, ადმინისტრირების პროგრამული საშუალების ცენტრალიზებული ინსტალირება/განახლება/გაუქმება.
- ინფორმაციის ცენტრალიზებული შეგროვება და ანგარიშების შედგენა ანტივირუსული დაცვის მდგომარეობის შესახებ.
- სერვერსა და კლიენტს შორის დაცული შეერთება, ადმინისტრირების აგენტის არსებობა.
- WEB კონსოლის არსებობა
- კლიენტების წინასწარი დარეგულირება და კონფიგურაციის ფაილების შენახვის შესაძლებლობა, შემდგომი გამოყენებისთვის (განახლების პროფილები, აკრძალული საიტები, დაგეგმვის გრაფიკი და ა.შ)
- AD (Active Directory)-სთან სინქრონიზაციის გზით კომპიუტერების ჯგუფის ავტომატურად შექმნის შესაძლებლობა.
- SIEM მხარდაჭერის მოდულის არსებობას;
- ანტივირუსის კლიენტის ადმინისტრირების აგენტის დაყენების სხვადასხვა შესაძლებლობა: ლოკალურად, ელ-ფოსტის გამოყენებით, Push ან გარე წამკითხავი USB მოწყობილობიდან .
- ოპერაციული სისტემებისთვის აგენტის შესაბამისი დასაყენებლი პაკეტის ავტომატური ან ხელის რეჟიმში არჩევის შესაძლებლობა.
- დაუცველი სამუშაო კომპიუტერების ავტომატური პოვნა, ქსელის ტოპოლოგიის მიხედვით.
- კომპიუტერის მდგომარეობის შესახებ ინფორმაციის შეგროვების შესაძლებლობა (გამოყენებული პროგრამები, სერვისები, პროცესები, ქსელური შეერთებები და სხვა) და ინფორმაციის ავტომატური შედარება დროის ინტერვალის მიხედვით, ასევე ცვლილებების შეტანის შესაძლებლობა (პროცესების და დრაივერების შეჩერება, სისტემური ფაილების და რეგისტრების წაშლა/აღდგენა) რომელიც უზრუნველყოფს კომპიუტერის სისტემის ნორმალურ ფუნქციონირებას.
- მოშორებული ინსტალირების შესაძლებლობა შემდეგ ოპერაციულ სისტემებზე - Windows , Linux
- მოშორებული ადმინისტრირების სერვერთან კონსოლის მიერთების შესაძლებლობა მომხმარებლის დომენური სახელისა და პაროლის გამოყენებით.
- მომხმარებელთა ანტივირუსული ბაზის განახლების საშუალება, როგორც შიდა ქსელის ადმინისტრირების სერვერის, ასევე ინტერნეტის საშუალებით;
- საჭიროებისამებრ ანტივირუსის ბაზების განახლების უკან დაბრუნება როგორც ცალკეული კომპიუტერებისთვის ასევე ჯგუფებისთვის.
- ქსელის ტრაფიკის ეკონომიის მიზნით სარკისებრი განახლების შესაძლებლობა ნებისმიერ კომპიუტერზე, განახლების გავრცელება ორი გზით HTTP და SMB.

- ცენტრალიზებული მართვის სერვერის თავსებადობა: Windows Server 2019, 2016, 2012/R2, 2008/R2, Windows 10
- შემდეგი მონაცემთა ბაზის მხარდაჭერა: MS SQL, MySQL
- Windows Failover Clustering მხარდაჭერა
- ლოგ ფაილების ექსპორტირება CSV, PDF ფორმატებში.

მოთხოვნები Microsoft Exchange საფოსტო სერვერის და საფოსტო ყუთების ანტივირუსული დაცვის უზრუნველსაყოფად:

ანტივირუსული დაცვის პროგრამას უნდა ქონდეს შემდეგი ოპერაციული სისტემების მხარდაჭერა: Microsoft Windows Server 2008, 2012, 2016, 2019. პროგრამების მხარდაჭერა: Microsoft Exchange Server 2013 , 2016, 2019

- ანტივირუსული დაცვა სერვერული ოპერაციული სისტემისთვის რომელზეც დაყენებული Microsoft Exchange-ის საფოსტო სერვერი.
- საფოსტო ტრაფიკის ანტივირუსული დაცვის პროგრამული საშუალებები
- არასასურველი (SPAM) წერილებისგან დაცვა
- მიბმული ფაილების ფილტრაციის შესაძლებლობა ფაილის ტიპის მიხედვით.
- თეთრი (whitelist) და შავი (blacklist) სიების ფუნქციონალური მოდულების არსებობა.
- საფოსტო წერილების ლოკალური კარანტინის შემოწმება და მართვა ვებ ინტერფესისი საშუალებით.
- ანტივირუსის ბაზების სიგნატურული განახლება და ასევე ანტივირუსის ძრავის განახლების საშუალება.
- ანტივირუსული პროგრამული უზრუნველყოფის სალიცენზიო ფაილი(გასაღები) **1800** მეილბოქსზე, ასევე მომხმარებლის სახელი, პაროლი და სერიული ნომერი.

Microsoft Exchange-ისთვის ანტივირუსული პროგრამული საშუალებას Windows-ის მართვის ქვეშ გააჩნდეს შემდეგი ფუნქციონალი:

- ელ-წერილების მრავალნაკადიანი სკანირების მხარდაჭერა
- ელ-წერილები ფილტრაცია SMTP-სერვერის დონეზე
- ანტისპამის შიდა შეფასების მაჩვენებლების ცვლილებების შესაძლებლობა, დეტექციის გაუმჯობესებისთის.
- ანტისპამი უნდა იყენებდეს შემდეგ ტექნოლგიებს (RBL, DNSBL, Fingerprinting, Reputation checking, Content analysis, Bayesian filtering, Rules, Manual whitelisting/blacklisting.
- ტრაფიკის ანტივირუსული სკანირება შემდეგი პროტოკოლებით : FTP, HTTP, HTTPs, POP3 ,POP3s, IMAP,IMAPs
- ელ-წერილების სკანირება მავნე კოდის შემცველობაზე
- რეზიდენტული ანტივირუსული მონიტორინგი
- ანტივირუსის სკანირება განრიგის ან ადმინისტრატორის ბრძანების მიხედვით.
- შემდეგი ტიპის ფაილების შემოწმება და განკურნვა: PKLITE, LZEXE, DIET, EXEPACK
- შემდეგი არქივირებული ფაილების ტიპების შემოწმება და განკურნვა: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE;
- ელ-წერილების ფილტრაციის შესაძლებლობა სხვადახვა მიბმული ფაილური ტიპის მიხედვით.
- ანტისპამი - „შავი“ და „თეთრი“ სიების არსებობა და ასევე „ნაცრისფერი“ სია რომელიც იცავს მომხმარებლებს სპამისგან იმ მეთოდის საშუალებით რომელიც ეფუძნება RFC821 სპეციფიკაციას.

- ფილტრაციის და ვერიფიკაციის შესაძლებლობა შემდეგი მეთოდებით: Approved IP list, Blocked IP list , Ignored IP list, Blocked Body Domain list, Ignored Body Domain list , Blocked Body IP list, Ignored Body IP list, Approved Senders list, Approved Senders list , Blocked Senders list, Approved Domain to IP list, Blocked Domain to IP list, Ignored Domain to IP list, Blocked countries list
    - ინტეგრაცია Windows-ის უსაფრთხოების ცენტრთან, Windows-ის განახლების ცენტრთან (სისტემის აქტუალური და კრიტიკული განახლებების არსებობის შემოწმება და მათი ამორჩევითი ინსტალაცია)
    - პროაქტიული დაცვა სხვადასხვა ტიპის ვირუსული საშიშროებისგან viruses, rootkits, worms spyware
    - ყველანაირი სკრიპტების შემოწმება: WSH, JavaScript, Visual Basic Script და სხვა.
    - Windows Management Instrumentation-ის მხარდაჭერა
    - სერვერის მდგომარეობის შესახებ ინფორმაციის შეგროვების შესაძლებლობა (გამოყენებული პროგრამები, სერვისები, პროცესები, ქსელური შეერთებები და სხვა)
    - მოვლენათა ჟურნალის არსებობა და შემოწმების შესაძლებლობა

სენდბოქს სერვისი/ლიცენზია - ანტივირუსის პროგრამული პაკეტების დაცვის დამატებითი მოდულის ლიცენზია

- ანტივირუსის პროდუქტის დაცვის დამატებითი მოდულის (ე.წ. სენდბოქსი) ლიცენზია რომელიც ინტეგრირდება ანტივირუსი ცენტრალიზებული მართვის სისტემაში, კომპიუტერების, სერვერების და ელ-ფოსტის დამატებითი დაცვის უზრუნველსაყოფად.
- პროდუქტი უნდა იყენებდეს მანქანური სწავლების და ქლაუდ სენდბოქსის ტექნოლოგიას, უცნობი საფრთხეებისაგან (ე.წ. 0-day) გაუმჯობესებული და ოპტიმიზირებული დაცვის მიზნით, ქცევის ანალიზის მიხედვით.
- შედმეგი ტიპის ფაილების შემოწმების შესაძლებლობა: docx, .xslx, .rtf , exe, dll, sys, jar, lnk, reg, msi swf, bat, .cmd, .js, .vbs, .ps და სხვა.
- თითოეულ შემოწმებული ფაილზე უნდა მოხდეს ანგარიშის წარმოდგენა, რომელიც უნდა შეიცავდეს დეტალურ ინფორმაციას (დასახელება, კატეგორია, კომპიუტერი) და მახასიათებლებს (ზომა, ჰეში) ამ საეჭვო ფაილის შესახებ, მდგომარეობა და სტატუსი
- ასევე ამ ინფორმაციის გადაცემა უნდა მოხდეს ცენტრალიზებული მართვის სისტემაში.

კრიპტოგრაფიული უსაფრთხოების SSL სერტიფიკატი ტექნიკური მოთხოვნები:

- 1 ერთეული მულტი დომენური (Multi-Domain) კრიპტოგრაფიული უსაფრთხოების (SSL) სერტიფიკატი **15** დომეინის/ქვედომეინის მხარდაჭერით.
- 2048-bit და 256-bit შიფრაციის მხარდაჭერა.
- SSL v3/TLS თავსებადობა
- MS Exchange Mail Server-ის და შემდეგი სერვისების მხარდაჭერა OWA, SMTP, Autodiscovery, ActiveSync
- CA-ს მხრიდან დომეინის მფლობელისა და ორგანიზაციის იდენტურობის შემოწმება.
- სერტიფიკატის მწარმოებლის გარანტია - მინიმუმ $1 000 000
- ნამდვილობის ვადა 1 წელი
- სერტიფიკატის ადმინისტრირების შესაძლებლობა მწარმოებლის ვებ გვერდზე, SSL სერტიფიკატის მართვა ვებ მენეჯმენტის საშუალებით.

შენიშვნა: SSL სერტიფიკატის სამართავად ვებ მენეჯმენტის საშუალებით, შემსყიდველს უნდა გადაეცეს აღნიშნულის SSL სერტიფიკატი მის account-ში რომელიც დარეგისტრირებული იქნება SSL სერტიფიკატის მწარმოებლის ვებ გვერდზე.

- სატენდერო წინადადებით წარმოდგენილი პროდუქტების შესაბამისობის დადგენა სატენდერო დოკუმენტაციაში ზემოთ მითითებულ მოთხოვნებთან მოხდება პროდუქტის მწარმოებლის ოფიციალურ ვებ–გვერდებზე განთავსებულ ინფორმაციაზე დაყრდნობით.

- შესყიდვის ობიექტი უნდა აკმაყოფილებდეს ტექნიკური დავალებით განსაზღვრულ მოთხოვნებს

- შესყიდვის ობიექტი უნდა აკმაყოფილებდეს ტექნიკური დავალებით განსაზღვრულ მოთხოვნებს
- შემსყიდველი შესყიდვის ობიექტის მიწოდების პარალელურად განახორციელებს შესყიდვის ობიექტის შემოწმებას, იმ შემთხვევაში თუ მიწოდებული ლიცენზიას შემოწმების პროცესში აღმოაჩნდება გარკვეული ხარვეზები შემსყიდველი უფლებამოსილია უარი განაცხადოს შესყიდვის ობიექტის მიღებაზე და მიღება-ჩაბარების აქტის გაფორმებაზე.
- შესყიდვის ობიექტის ტექნიკური და ხარისხობრივი კონტროლი (შემოწმება) გაიმართება შემსყიდველის იურიდიულ მისამართზე, მიმწოდებელი ორგანიზაციის წარმომადგენლ(ებ)ის თანდასწრებით.
- ანგარიშსწორება განხორციელდება შესყიდვის ობიექტის მიწოდების შემდეგ მხარეთა შორის მიღება ჩაბარების აქტის გაფორმებიდან **7** (შვიდი) დღეში (წინასწარი, საავანსო გადახდა ელექტრონულ ტენდერში არ გამოიყენება).
- სახელმწიფო შესყიდვის დაფინანსების წყაროა: **100 %** - სახელმწიფო ბიუჯეტი (2021 წლის სახსრები).

შესყიდვის ობიექტის სავარაუდო ღირებულებაა - ლარი

მოთხოვნები ანტივირუსის მომწოდებლის პრეტენდენტის მიმართ

ა) პრეტენდენტი უნდა იყოს ანტივირუსის მწარმოებლის ოფიციალური პარტნიორი საქართველოში წარმოდგენილ უნდა იქნას ანტივირუსის მწარმოებლის პარტნიორობის დამადასტურებელი სერტიფიკატი.

ბ) პრეტენდენტის გამოცდილების აღნიშნულ საქმიანობის სფეროში დამადასტურებელი დოკუმენტაცია. პრეტენდენტმა უნდა წარმოადგინოს **შესაბამისი და/ან მსგავსი შესყიდვის ობიექტის მიწოდების** დამადასტურებელი დოკუმენტაცია, **რომლის საერთო ღირებულება უნდა შეადგენდეს არანაკლებ - 10 000 (ათიათასი) ლარს.** პრეტენდენტმა, გამოცდილების დასადასტურებლად, უნდა წარმოადგინოს (სისტემაში ატვირთოს, გაფორებული შესაბამისი ხელშეკრულებების ასლები, შესყიდვის ობიექტის მიწოდების დამადასტურებელი დოკუმენტის ასლები (მიღება-ჩაბარების აქტი, სასაქონლო ზედნადები ან/და სხვა შესაბამისი დამადასტურებელი დოკუმენტი) - იმ შემთხვევაში თუ პრეტენდენტს შესაბამისი და/ან მსგავსი შესყიდვის ობიექტის დამადასტურებელი დოკუმენტაცია განთავსებულია შესყიდვების ერთიან ელექტრონულ სისტემაში (https://tenders.procurement.gov.ge/) მაშინ პრეტენდენტის მიერ შესაძლებელია წარმოდგენილი იქნას შესაბამისი NAT, SPA და/ან CMR ნომრები. **შესაბამის და/ან მსგავსი შესყიდვის ობიექტის მიწოდების სფეროში გამოცდილების არ ქონა გამოიწვევს პრეტენდენტის დისკვალიფიკაციას.**