1. ანტივირუსის პროგრამული პაკეტების სახელმწიფო შესყიდვა

ელექტრონული ტენდერის*

*-ელექტრონული ტენდერი (ელექტრონული ვაჭრობის დაფარული მონაცემებით, დამატებითი რაუნდების გარეშე აბრევიატურით NAT)

(წინამდებარე დოკუმენტაციაში მოცემულია შესყიდვების ელექტრონულ სისტემაში ელექტრონულად შესავსები სატენდერო პირობები)

კლასიფიკატორის CPV კოდი №48761000 - ანტივირუსის პროგრამული პაკეტები

თბილისი

2022 წელი

2. ტექნიკური მოთხოვნები როგორც იურიდიული ასევე ფიზიკური პირებისათვის: პრეტენდენტმა ტექნიკური დოკუმენტაციის სახით სისტემაში უნდა ატვირთოს შემდეგი დოკუმენტები და ინფორმაცია:

ა) პრეტენდენტის მიერ წარმოდგენილი უნდა იყოს ფასების ცხრილი (იხ. დანართი №1 - Excel-ის ფორმატში ან პრეტენდენტის მიერ ფასების ცხრილი წარმოდგენილი უნდა იყოს PDF ფორმატში ელექტრონულად ხელმოწერილი ან/და დამოწმებული ელექტრონული შტამპით) **სადაც მითითებული უნდა იყოს ანტივირუსის პროგრამული პაკეტების მწარმოებლის ან/და ბრენდის* დასახელება (ძირითადი მახასიათებლები, აღწერილობა) და პროგრამული პაკეტების ერთეულის და საერთო ფასები** (აღნიშნულის წარმოუდგენლობა დაზუსტებას არ დაექვემდებარება და გამოიწვევს პრეტენდეტის დისკვალიფიკაციას) სატენდერო წინადადებაში ერთეულის და საერთო ფასი გამოსახული უნდა იყოს შესყიდვის ობიექტის მიწოდებასთან დაკავშირებული ხარჯების და საქართველოს კანონმდებლობით გათვალისწინებული ყველა გადასახადის გათვალისწინებით).

**- მწარმოებლის ან/და ბრენდის წარმოდგენა სავალდებულოა, რათა შესაძლებელი იყოს იდენტიფიკაცია და შესაბამისობა შემოთავაზებული საქონლის სატენდერო მოთხოვნებთან.*

ბ) პრეტენდენტი უნდა იყოს ანტივირუსის და SSL სერტიფიკატის მწარმოებლის ოფიციალური პარტნიორი საქართველოში და წარმოდგენილ უნდა იქნას ანტივირუსის და SSL სერტიფიკატის მწარმოებლების პარტნიორობის დამასტურებელი სერტიფიკატები - ქართულ ენაზე ნათარგმნი და სანოტარო წესით დამოწმებული.

გ) პრეტენდენტის გამოცდილების აღნიშნულ საქმიანობის სფეროში დამადასტურებელი დოკუმენტაცია. პრეტენდენტმა უნდა წარმოადგინოს შესაბამისი შესყიდვის ობიექტის მიწოდების დამადასტურებელი დოკუმენტაცია, რომლის საერთო ღირებულება უნდა შეადგენდეს არანაკლებ - **50 000 (ორმოცდაათიათასი)** 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 CMR ან და სხვა შესაბამისი ნომრები. **შესაბამის შესყიდვის ობიექტის მიწოდების სფეროში გამოცდილების არ ქონა გამოიწვევს პრეტენდენტის დისკვალიფიკაციას.**

დ) პრეტენდენტის მიერ წარმოდგენილი უნდა იყოს ხელმძღვანელის და საკონტაქტო პირის სახელი და გვარი და საბანკო რეკვიზიტები - აღნიშნული ინფორმაცია წარმოდგენილი უნდა იყოს იმ შემთხვევაში, თუ პრეტენდენტის მიერ შესყიდვების ერთიან ელექტრონულ სისტემაში პრეტენდენტის პროფილში არ არის და/ან არასრულად არის შევსებული შესაბამისი ინფორმაცია.

შენიშვნა:

- **ტენდერთან დაკავშირებული ყველა დოკუმენტი ან/და ინფორმაცია წარმოდგენილი უნდა იქნას ქართულ ენაზე. დოკუმენტების ან/და ინფორმაციის უცხოურ ენაზე წარდგენის შემთხვევაში მას უნდა დაერთოს სანოტარო წესით დამოწმებული ქართულენოვანი თარგმანი.**
- სახელმწიფო შესყიდვების ერთიან ელექტრონულ სისტემაში ატვირთული დოკუმენტები და/ან ინფორმაცია (რომელიც ითვალისწინებს ხელმოწერას) უნდა იქნას ელექტრონულად ხელმოწერილი შესაბამისად უფლებამოსილი პირის მიერ ან დამოწმებული კვალიფიციური ელექტრონული შტამპით, მოქმედი კანონმდებლობის ფარგლებში.
- შესყიდვების ერთიან ელექტრონულ სისტემაში „მიმწოდებლად“ რეგისტრირებული არარეზიდენტი მომხმარებლები განთავისუფლებულები არიან „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონის მე-3 მუხლის მე-3 პუნქტით გათვალისწინებული ვალდებულებისაგან იხ. საქართველოს მთავრობის განკარგულება.
- **პრეტენდენტს არ აქვს უფლება წარმოადგინოს ალტერნატიული სატენდერო წინადადება.**
- შესყიდვის ობიექტის სპეციფიკის გათვალისწინებით ვინაიდან შესყიდვის ობიექტს წარმოადგენს ანტივირუსის პროგრამული პაკეტების შესყიდვა) შესაბამისი პროგრამული პაკეტების მწარმოებელმა ან/და გამყიდველმა ორგანიზაციამ, ასევე შესაბამისი გამოცდილების მქონე პრეტენდენტმა შესაძლებელია ანტივირუსული პროგრამული პაკეტების გაყიდვა განახორციელოს საბაზრო ღირებულებასთან შედარებით დაბალ ფასად. აღნიშნულიდან გამომდინარე, პრეტენდენტის მიერ სისტემაში შესყიდვის ობიექტის სავარაუდო ღირებულებასთან 20%-ით და/ან მეტით დაბალი საბოლოო ფასის დაფიქსირების შემთხვევაში არ წარმოეშვება ფასწარმოქმნის ადეკვატურობის დასაბუთების ვალდებულება. აღნიშნულიდან გამომდინარე, პრეტენდენტის მიერ სისტემაში შესყიდვის ობიექტის სავარაუდო ღირებულებასთან 20%-ით და/ან მეტით დაბალი საბოლოო ფასის დაფიქსირების შემთხვევაში არ წარმოეშვება ფასწარმოქმნის ადეკვატურობის დასაბუთების ვალდებულება.

აღნიშნულიდან გამომდინარე, პრეტენდენტის მიერ სისტემაში შესყიდვის ობიექტის სავარაუდო ღირებულებასთან 20%-ით და/ან მეტით დაბალი საბოლოო ფასის დაფიქსირების შემთხვევაში არ წარმოეშვება ფასწარმოქმნის ადეკვატურობის დასაბუთების ვალდებულება.

- სატენდერო დოკუმენტაციასთან დაკავშირებული განმარტებებისა და დამატებითი ინფორმაციის მოთხოვნა ნებისმიერ დაინტერესებულ პირს შეუძლია სახელმწიფო შესყიდვების ერთიანი ელექტრონული სისტემის მოდულის „კითხვა/პასუხის“ მეშვეობით შესაბამის ტენდერში „ტენდერი გამოცხადებულია“ სტატუსის მინიჭებიდან „წინადადების მიღება დასრულებულია“ სტატუსის მინიჭებამდე არაუგვიანეს 24 საათისა.
- ტენდერთან დაკავშირებული განმარტებისა და დამატებითი ინფორმაციის დაზუსტება/განმარტება განხორციელდება გონივრულ ვადაში, მაგრამ არაუგვიანეს 2 საათისა შესაბამის ტენდერში „წინადადების მიღება დასრულებულია“ სტატუსის მინიჭებამდე.
- ყველაზე დაბალი ფასის წინადადების მქონე მიმწოდებლის მოთხოვნის შემთხვევაში პუნქტით გათვალისწინებული შესაბამისი დაზუსტება/განმარტება განხორციელდება გონივრულ ვადაში, შესაბამის ტენდერში „შერჩევა/შეფასების“ სტატუსის მინიჭებიდან „ხელშეკრულება დადებულია“ სტატუსის მინიჭებამდე.
- სატენდერო დოკუმენტაციასთან დაკავშირებული განმარტებებისა და დამატებითი ინფორმაციის გაცემაზე უფლებამოსილი პირია სატენდერო კომისიის აპარატის წევრი - გიორგი ფირცხალავა, ტელ: 2 40 91 45 - შესყიდვების სამსახურის შესყიდვების სპეციალისტი;

3. შესყიდვის ობიექტის მიწოდების ვადა და ტექნიკური დავალება:

3.1 მიმწოდებელმა უნდა უზრუნველყოს შესყიდვის ობიექტის მიწოდება ხელშეკრულების გაფორმებიდან 7 (შვიდი) კალენდარულ დღეში.

3.2 მოწოდებული პროგრამული პაკეტების ლიცენზიების მოქმედების ვადა უნდა იყოს 1 (ერთი) წელი;

3.3 **შესყიდვის ობიექტია:** ანტივირუსული პროგრამული პაკეტის 1 (ერთი) წლიანი ლიცენზია **1000** მომხმარებელზე/მოწყობილობაზე (სერვერული სისტემისათვის და საოფისე კომპიუტერისათვის), ანტივირუსული/ანტისპამ დაცვა Microsoft Exchange სერვერსითვის **550** ელ-ფოსტის მეილბოქსზე, სენდბოქს სერვისი/ლიცენზია **550** მომხმარებელზე და **1 ცალი** მულტიდომენური კრიპტოგრაფიული უსაფრთხოების SSL სერტიფიკატი.

შენიშვნა: – შემსყიდველს ამ ეტაპზე შეძენილი აქვს ანტივირუსული პროგრამული პაკეტის 1 (ერთი) წლიანი ლიცენზია 900 მომხმარებელზე/მოწყობილობაზე (სერვერული სისტემისათვის და საოფისე კომპიუტერისათვის), ანტივირუსული/ანტი სპამ დაცვა Microsoft Exchange სერვერსითვის 1800 ელ-ფოსტის მეილბოქსზე, 1 ცალი კრიპტოგრაფიული უსაფრთხოების SSL სერტიფიკატი და სენდბოქს სერვისი/ლიცენზია 700 მომხმარებელზე. (იხ. **NAT210005993**) რომლის მოქმედების ვადა იწურება 2022 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). **სხვა ანტივირუსული პროგრამული პაკეტის შემოთავაზების შემთხვევაში მიმწოდებელმა უნდა უზრუნველყოს შესაბამისი ინსტალაცია კომპიუტერულ მოწყობილობებზე.**

3.4 ანტივირუსული პროგრამა უნდა უზრუნველყოფდეს:

სერვერული და საოფისე სისტემებისათვის

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

•თავსებადობა Microsoft Windows-ის სერვერულ ოპერაციულ სისტემებთან: Windows Server 2019, 2016, 2012, 2012 R2, 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.

•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 მონიტორინგი 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 - ინფორმაციის 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 პრიორიტეტულობის 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.
- 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 სალიცენზიო ფაილი(გასაღები) 1000 მომხმარებელზე (სამუშაო კომპიუტერებისათვის და სერვერებისათვის), ასევე მომხმარებლის სახელი, პაროლი და სერიული ნომერი.
- შესაძლებელი უნდა იყოს ანტივირუსის გამოყენება/ინსტალირება როგორც ცენტრალიზებული მართვით ასევე მის გარეშე ცალკეულად ლიცენზიის გამოყენებით.

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) **550** 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 სასურველია „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 5 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

- მოწოდებული ანტივირუსული პროგრამული პაკეტები უნდა იყოს ერთიდაიმავე მწარმოებლის.

- 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 (2022 წლის სახსრები).

შესყიდვის ობიექტის სავარაუდო ღირებულებაა – ლარი

პრეტენდენტის დასახელება: _____; მისამართი: _____; ტელ: _____;
ელ. ფოსტა: _____ და საბანკო რეკვიზიტები_____;

N	შესყიდვის ობიექტის (ანტივირუსის პროგრამული პაკეტის) დასახელება	ლიცენზიის ვადა	შესყიდვის ობიექტის მწარმოებლის ან/და ბრენდის დასახელება	რაოდენობა	ერთეულის ფასი (ლარი)	საერთო ღირებულება (ლარი)
1	საოფისე კომპიუტერებისთვის და სერვერული სისტემისათვის ანტივირუსული პროგრამის ლიცენზია	1 წელი		1000		- ₾
2	ანტივირუსული/ანტისპამ დაცვა Microsoft Exchange სერვერსითვის ელ-ფოსტის მეილბოქსზე	1 წელი		550		- ₾
3	სენდბოქს სერვისი/ლიცენზია	1 წელი		550		- ₾
4	მულტიდომენური კრიპტოგრაფიული უსაფრთხოების SSL სერტიფიკატი	1 წელი		1		- ₾
					ჯამი:	- ₾

შენიშვნა: ფასების ცხრილის შესაბამის გრაფაში უნდა იყოს მითითებული ანტივირუსული პროგრამული პაკეტების მწარმოებლის ან/და ბრენდის დასახელება, ერთეულისა და საერთო ფასები (აღნიშნულის წარმოუდგენლობა დაზუსტებას არ დაექვემდებარება და გამოიწვევს პრეტენდეტის დისკვალიფიკაციას).

*- მწარმოებლის ან/და ბრენდის წარმოდგენა სავალდებულოა, რათა შესაძლებელი იყოს იდენტიფიკაცია და შესაბამისობა შემოთავაზებული პროდუქტის, სატენდერო მოთხოვნებთან.

პრეტენდენტის ხელმოწერა _____
(თანამდებობა და ხელმოწერა**)

** - პრეტენდენტის მიერ ფასების ცხრილი წარმოდგენილი უნდა იყოს Excel-ის ფორმატში ან/და ფასების ცხრილი წარმოდგენილი უნდა იყოს PDF ფორმატში ელექტრონულად ხელმოწერილი ან/და დამოწმებული ელექტრონული შტამპით.

4. სახელმწიფო შესყიდვების შესახებ ხელშეკრულების პროექტი

ქ. თბილისი **ხელშეკრულება N** 2022 წელი

წინამდებარე დოკუმენტი წარმოადგენს სახელმწიფო შესყიდვების შესახებ ხელშეკრულების პროექტს, რომელიც დაიდება ელექტრონული ტენდერის ჩატარების შედეგად. წინამდებარე ხელშეკრულების პროექტის პირობების დაზუსტება განხორციელდება გამარჯვებული პრეტენდენტის სატენდერო წინადადების შესაბამისად, რომელიც ამავდროულად თანდართული ექნება ხელშეკრულებას, როგორც მისი განუყოფელი ნაწილი.

1. ხელშეკრულების დამდები მხარეები

ერთის მხრივ სსიპ საზოგადოებრივი მაუწყებელი (შემდგომში ,,შემსყიდველი") მისი გენერალური დირექტორის თინათინ ბერძენიშვილის სახით და მეორეს მხრივ, ———————— (შემდგომში ,,მიმწოდებელი") მისი დირექტორის ———————— სახით, სახელმწიფო შესყიდვების კანონის და პრეტენდენტის (მისი დასახელება) სატენდერო წინადადების საფუძველზე, ელქტრონული ტენდერის ჩატარების შედეგად დებენ წინამდებარე სახელმწიფო შესყიდვის შესახებ ხელშეკრულებას შემდეგზე: შემსყიდველმა ჩაატარა ელექტრონული ტენდერი (**NAT----------**) ანტივირუსის პროგრამული პაკეტების სახელმწიფო შესყიდვაზე (კლასიფიკატორის CPV კოდი №48761000 - ანტივირუსის პროგრამული პაკეტები), რომელშიც გამარჯვებულად მიჩნეულ იქნა მიმწოდებლის სატენდერო წინადადება და მიმწოდებელმა აიღო ვალდებულება გაუწიოს მომსახურება შემსყიდველს.

1. ქვემოთ ჩამოთვლილი დოკუმენტები ქმნიან მოცემულ ხელშეკურულებას და წარმოადგენენ მის განუყოფელ ნაწილს:

ა) წინამდებარე ხელშეკრულება;

ბ) პრეტენდენტის მიერ წარმოდგენილი სატენდერო წინადადება და სატენდერო წინდადებაზე თანდართული ყველა სხვა დოკუმენტი;.

გ) სატენდერო დოკუმენტაცია;

2. ხელშეკრულებაში გამოყენებულ ტერმინთა განმარტებები

2.1. „ხელშეკრულება სახელმწიფო შესყიდვის შესახებ" (შემდგომში _ „ხელშეკრულება") _ შემსყიდველსა და მიმწოდებელს შორის დადებული წინამდებარე ხელშეკრულება, რომელიც ხელმოწერილია მხარეთა მიერ, მასზე თანდართული ყველა დოკუმენტით.

2.2. „ხელშეკრულების ღირებულება" _ საერთო თანხა, რომელიც უნდა გადაიხადოს შემსყიდველმა მიმწოდებლის მიერ ხელშეკრულებით ნაკისრი ვალდებულებების სრული და ზედმიწევნით შესრულებისათვის.

2.3. „დღე", „კვირა", „თვე" _ კალენდარული დღე, კვირა, თვე.

2.4. „შემსყიდველი" – ორგანიზაცია, რომელიც ახორციელებს შესყიდვას.

2.5. „მიმწოდებელი" – პირი, რომელიც ახორციელებს შესყიდვის ობიექტის მიწოდებას ხელშეკრულების ფარგლებში.

3. ხელშეკრულების საგანი

3.1. ანტივირუსის პროგრამული პაკეტების შესყიდვა.

3.2. ხელშეკრულებით გათვალისწინებული შესყიდვის ობიექტის აღწერა მოცემულია სატენდერო დოკუმენტაციაში.

4. ხელშეკრულების ღირებულება

4.1. ხელშეკრულების ჯამური ღირებულება შეადგენს ————————————ლარს.

4.2. ხელშეკრულების ჯამური ღირებულება მოიცავს ხელშეკრულებით გათვალისწინებული შესყიდვის ობიექტის მიწოდებასთან დაკავშირებულ მიმწოდებლის ყველა ხარჯს.

5. ხელშეკრულების შესრულების კონტროლი

5.1 მიმწოდებლის მიერ ხელშეკრულებით ნაკისრი ვალდებულების შესრულების კონტროლს შემსყიდველის მხრიდან განახორციელებს - სსიპ „საზოგადოებრივი მაუწყებლის" სპეციალურად უფლებამოსილი თანამშრომელ(ებ)ი.

5.2 შემსყიდველი საქონლის მიწოდების პარალელურად განახორციელებს საქონლის შემოწმებას, იმ შემთხვევაში თუ მიწოდებულ საქონელს შემოწმების პროცესში აღმოჩნდება გარკვეული ხარვეზები ან შემოწმებული საქონელი ვერ დაკმაყოფილებს შესაბამის ტექნიკურ მონაცემებს, შემსყიდველი უფლებამოსილია უარი განაცხადოს შესყიდვის ობიექტის მიღებაზე და მიღება-ჩაბარების აქტის გაფორმებაზე.

5.3 მიწოდებული საქონლის ტექნიკური შემოწმების პროცესში მიმწოდებელი ვალდებულია საკუთარი ხარჯებით უზრუნველყოს კონტროლის (ინსპექტირების) შედეგად გამოვლენილი წუნდებული საქონლის შეცვლა.

5.4 შესყიდვის ობიექტის ტექნიკური და ხარისხობრივი კონტროლი (შემოწმება) გაიმართება შემსყიდველის იურიდიულ მისამართზე, მიმწოდებელი ორგანიზაციის წარმომადგენლ(ებ)ის თანდასწრებით.

6. შესყიდვის ობიექტის მიღება-ჩაბარების წესი

6.1 მიმწოდებელმა წინამდებარე ხელშეკრულებით გათვალისწინებული შესყიდვის ობიექტის მიწოდება უნდა განახორციელოს ხელშეკრულების გაფორმებიდან 5 (ხუთი) კალენდარულ დღეში.
6.2 შესყიდვის ობიექტის მიწოდების ადგილია ქ. თბილისი, კოსტავას ქ. N68;
6.3 შესყიდვის ობიექტის მიღება-ჩაბარება განხორციელდება ანტივირუსული პროგრამული პაკეტის მიწოდების შემდეგ, შემსყიდველისა და მიმწოდებლის უფლებამოსილი წარმომადგენლების მიერ მიღება-ჩაბარების აქტის გაფორმებით (შემსყიდველის მხრიდან მიღება-ჩაბარების აქტის გაფორმებაზე უფლებამოსილ პირს წარმოადგენს წინამდებარე ხელშეკრულების სპეციფიკური პირობების 5.1 მუხლში მითითებული პირ(ებ)ი.
6.4 შესყიდვის ობიექტის მიწოდების პარალელურად მიმწოდებელმა უნდა უზრუნველყოს შემსყიდველისათვის შესაბამისი საგადასახადო დოკუმენტაციის წარმოდგენა.
6.5 შესყიდვის ობიექტი ჩაითვლება მიღებულად მხოლოდ მიღება-ჩაბარების აქტის გაფორმების შემდეგ.

7. გარანტია

7.1 მიმწოდებელი იღებს ვალდებულებას, რომ გაწეული მომსახურების ხარისხი უპასუხებს ხელშეკრულებით გათვალისწინებულ პირობებს და დააკმაყოფილებს შემსყიდველის მოთხოვნებს.
7.2 გაწეული მომსახურების ხარისხი უნდა შეესაბამებოდეს ამ სფეროში არსებულ სტანდარტებს და ტექნიკურ ნორმებს.

8. ანგარიშსწორება

8.1 ანგარიშსწორება მოხდება ლარში;
8.2 გადახდის ფორმა - უნაღდო;
8.3 ანგარიშსწორება განხორციელდება შესყიდვის ობიექტის მიწოდების შემდეგ, მხარეთა შორის მიღება-ჩაბარების აქტის გაფორმებიდან 10 (ათი) დღეში, წინასწარი (საავანსო) გადახდა ელექტრონულ ტენდერში არ გამოიყენება.
8.4 სახელმწიფო შესყიდვის დაფინანსების წყაროა: 100 % სახელმწიფო ბიუჯეტის სახსრები ***(2022 წლის სახსრები)***

9. ფასები

9.1 ხელშეკრულებაში განსაზღვრული ფასის ცვლილება დასაშვებია მხოლოდ შემდეგ შემთხვევებში:
ა) საქართველოს სამოქალაქო კოდექსის 398-ე მუხლით გათვალისწინებული გარემოებების დადგომის შემთხვევაში (დაუშვებელია სახელმწიფო შესყიდვების შესახებ ხელშეკრულების ჯამური ღირებულების 10 %-ზე მეტი ოდენობით გაზრდა), ფასების ცვლილების შესახებ ხელშეკრულების მხარემ უნდა შეატყობინოს მეორე მხარეს წერილობით, რომელიც თავის მხრივ უფლებამოსილია არ დაეთანხმოს აღნიშნულ ცვლილებაზე.

10. ფორს-მაჟორი

10.1. ხელშეკრულების, რომელიმე მხარის მიერ ხელშეკრულების პირობების შეუსრულებლობა არ განიხილება ხელშეკრულების პირობების დარღვევად თუ შესრულების შეფერხება ან მისი ვალდებულებების შეუსრულებლობა არის ფორს-მაჟორული გარემოებების შედეგი;
10.2. ამ ხელშრეკრულების მიზნებისათვის ფორს-მაჟორი ნიშნავს მხარეებისათვის გადაულახავ და მათი კონტროლისაგან დამოუკიდებელ გარემოებებს, რომლებიც არ არიან მხარეების შეცდომებთან და დაუდევრობებთან და რომლებსაც გააჩნიათ წინასწარ გაუთვალისწინებელი ხასიათი. ასეთი გარემოება შეიძლება გამოწვეული იქნას ომით, ეპიდემიით;
10.3. ფორს-მაჟორული გარემოების დადგომის შემთხვევაში მხარემ, რომლისათვისაც შეუძლებელი ხდება ნაკისრი ვალდებულების შესრულება, დაუყოვნებლივ უნდა გაუგზავნოს მეორე მხარეს წერილობითი შეტყობინება ასეთი გარემოებების და მათი გამომწვევი მიზეზების შესახებ.

11. მხარეთა ურთიერთობა

11.1. ნებისმიერი ოფიციალური შეტყობინება მხარეთა შორის უნდა ატარებდეს წერილობით ფორმას. წერილობითი შეტყობინება, რომელსაც ერთი მხარე, ხელშეკრულების შესაბამისად, უგზავნის მეორე მხარეს იგზავნება საფოსტო გზავნილის სახით;
11.2. შეტყობინება ძალაში შედის ადრესატის მიერ მისი მიღების დღეს ან შეტყობინების ძალაში შესვლის დადგენილ დღეს, თუ ამ თარიღიდან რომელი უფრო გვიან დგება.

12. ხელშეკრულების პირობების შეუსრულებლობა

12.1 ხელშეკრულების ნაკისრი ვალდებულების შეუსრულებლობის და/ან არაჯეროვანი შესრულების შემთხვევაში, მიმწოდებელს ეკისრება პირგასამტეხლო, სახელშეკრულებო თანხის და/ან შეუსრულებელი ვალდებულების - **3 %** ოდენობით, რომლის გადახდა მიმწოდებელმა უნდა უზრუნველყოს შემსყიდველის წერილობითი მოთხოვნის მიღებიდან 5 (ხუთი) დღის განმავლობაში.
12.2 ხელშეკრულებით ნაკისრი ვალდებულებების ვადის გადაცილებისათვის მიმწოდებელს დაეკისრება პირგასამტეხლოს გადახდა, - ყოველ ვადაგადაცილებულ დღეზე ხელშეკრულების ღირებულების **0,02 %**-ის ოდენობით, ხოლო, თუკი ადგილი აქვს ვალდებულების ნაწილის შეუსრულებლობას, პირგასამტეხლო შეადგენს ვალდებულების შეუსრულებელი ნაწილის - **0.02 %**-ს.
12.3 გადახდის ვადის გადაცილების შემთხვევაში, მიმწოდებელი უფლებამოსილია დააკისროს შემსყიდველს პირგასამტეხლო, ყოველ ვადაგადაცილებულ დღეზე გადაუხდელი თანხის **0,02** %-ის ოდენობით.
12.4 პირგასამტეხლოს გადახდა არ ათავისუფლებს მხარეს ძირითადი ვალდებულებების შესრულებისაგან.

13. ხელშეკრულების შეწყვეტა

13.1 ხელშეკრულების დამდები ერთ-ერთი მხარის მიერ ხელშეკრულების პირობების შეუსრულებლობის შემთხვევაში მეორე მხარეს შეუძლია მიიღოს გადაწყვეტილება ხელშეკრულების სრული ან მისი ცალკეული პირობების მოქმედების შეწყვეტის შესახებ.

13.2 მიმწოდებლის მიერ ხელშეკრულებით ნაკისრი ვალდებულების შეუსრულებლობის და/ან არაჯეროვანი შესრულების შემთხვევაში (მათ შორის ვადების დარღვევის შემთხვევაში), აგრეთვე იმ შემთხვევაში თუ მიწოდებული საქონლის ხარისხი არ დააკმაყოფილებს ხელშეკრულებით განსაზღვრულ პირობებს და შემსყიდველის მიერ წუნდებული საქონლის შესაცვლელად დამატებით განსაზღვრულ ვადაში არ მოხდება წუნდებული საქონლის შეცვლა შემსყიდველი უფლებამოსილია ცალმხრივად შეწყვიტოს ხელშეკრულება და გამოიყენოს წინამდებარე ხელშეკრულებით გათვალისწინებული საჯარიმო სანქციები მოქმედი კანონმდებლობის შესაბამისად.

13.3 ხელშეკრულების დამდები მხარე, რომელიც მიიღებს 12.1 და 12.2 პუნქტებით გათვალისწინებულ გადაწყვეტილებას ვალდებულია შეატყობინოს მეორე მხარეს მიღებული გადაწყვეტილება, მისი მიღების საფუძველი და ამოქმედების თარიღი.

13.4 ხელშეკრულების ცალკეული პირობების მოქმედების შეწყვეტა არ ათავისუფლებს მხარეებს დანარჩენი ვალდებულების შესრულებისაგან.

13.5 ხელშეკრულების შეწყვეტა პირობების დარღვევის გამო არ ათავისუფლებს მიმწოდებელს ხელშეკრულების შეუსრულებლობისთვის გათვალისწინებული პასუხისმგებლობისაგან.

14. გადასახადები და ბაჟები

მიმწოდებელი პასუხს აგებს მომსახურების გაწევასთან დაკავშირებული ყველა იმ გადასახადის გადახდაზე, რომლებიც გადასახდელია საქართველოს ფარგლებში

15. დამატებითი პირობები

15.1. მხარეები პასუხს აგებენ ხელშეკრულებით ნაკისრი ვალდებულებების შეუსრულებლობისათვის და/ან არაჯეროვანი შესრულებისათვის საქართველოს კანონმდებლობით დადგენილი წესით;

15.2. წინამდებარე ხელშეკრულების ნებისმიერი ცვლილება ან დამატება ძალაშია მხოლოდ მას შემდეგ, რაც ის წერილობითი ფორმითაა შედგენილი და ხელმოწერილია მხარეთა მიერ;

15.3. ხელშეკრულება შედგენილია თანაბარი იურიდიული ძალის მქონე 2 (ორი) იდენტურ ეგზემპლიარად, თითო ყოველი მხარისთვის.

16. მხარეთა რეკვიზიტები:

შემსყიდველი:
სსიპ "საზოგადოებრივი მაუწყებელი"

ქ. თბილისი, კოსტავას ქ. #68
საიდენტიფიკაციო კოდი: 204 858 163

რეკვიზიტები:
დაფინანსების წყარო: სახელმწიფო ხაზინა
ხაზინის ერთიანი ანგარიში
კოდი: TRESGE22

გენერალური დირექტორი

თინათინ ბერძენიშვილი ----------