ხელშეკრულება საქონლის (თანმდევი მომსახურებით) შესყიდვის შესახებ # 60-7-219-5434

ქ. თბილისი 2019 წ. 25.11

I.მხარეები

1.1 წინამდებარე ხელშეკრულება დადებულია 2019 წლის 25.11----------, ერთის მხრივ სს „საქართველოს სახელმწიფო ელექტროსისტემას", წარმოდგენილი მისი მმართველთა საბჭოს წევრის დავით ვარდიაშვილი (მინდობილობა #181378706) სახით (შემდგომში – ,,შემსყიდველი") და მეორეს მხრივ შპს ,,იუჯითი" (შემდგომში– ,,მიმწოდებელი''), წარმოდგენილი დირექტორის ერმილე სულაძის სახით, შორის, რომლებიც მოქმედებენ საზოგადოების წესდებისა და მოქმედი კანონმდებლობის საფუძველზე.

II.ხელშეკრულების საგანი

2.1. ,,მიმწოდებელი" ვალდებულია ,,შემსყიდველს" მიაწოდოს საქონელი (თანმდევი მომსახურებით) (CPV კოდი : 48700000; 48760000) დანართი #1-is (ფასების ცხრილი) და დანართი #2–ის (საქონლის (თანმდევი მომსახურებით) ტექნიკური სპეციფიკაცია) შესაბამისად.

2.2 დანართი #1 და დანართი #2 წარმოადგენს წინამდებარე ხელშეკრულების განუყოფელ ნაწილს.

III.საქონლის (თანმდევი მომსახურებით) ღირებულება და ანგარიშსწორების პირობები

3.1. საქონლის (თანმდევი მომსახურებით) საერთო ღირებულება განსაზღვრულია წინამდებარე ხელშეკრულების დანართი #1-ის (ფასების ცხრილი) შესაბამისად და შეადგენს 308 900,54 (სამას რვა ათას ცხრაასი აშშ დოლარი და 54 ცენტი) აშშ დოლარს დღგ-ს ჩათვლით (შემდგომში – ,,ხელშეკრულების ღირებულება").

3.2 ანგარიშსწორება განხორციელდება ფაქტიურად მოწოდებულ საქონელზე (თანმდევი მომსახურებით) მიღება-ჩაბარების აქტის გაფორმებიდან და საგადასახადო ანგარიშ–ფაქტურის წარმოდგენიდან 8 (რვა) სამუშაო დღის განმავლობაში.

3.3. "შემსყიდველი" "მიმწოდებელს" უხდის საავანსო თანხას (,,ხელშეკრულების ღირებულების" არაუმეტეს 30%-ისა). ,,მიმწოდებლის" მხრიდან შესაბამისი ოდენობის საბანკო გარანტიის წარმოდგენის შემთხვევაში, საბანკო გარანტიის წარმოდგენიდან 5 (ხუთი) სამუშაო დღის განმავლობაში. საბანკო გარანტია ძალაში უნდა იყოს ხელშეკრულების მოქმედების ვადაზე არანაკლებ 30 (ოცდაათი) კალენდარული დღით მეტი ვადით. საბანკო გარანტიის შესაბამისი ანგარიშფაქტურა წარმოდგენილი უნდა იყოს ავანსის გადახდიდან 2 (ორი) სამუშაო დღეში. ავანსად გაცემული თანხა ჩაითვლება საბოლოო ანგარიშსწორებისას.

ვინაიდან, შპს „იუჯითი" რეგისტრირებულია თეთრ სიაში (სახელმწიფო შესყიდვების სააგენტოს თავმჯდომარის N4241, 24.11.2019წ. განკურგულება) სახელმწიფო შესყიდვების სააგენტოს თავმჯდომარის 2016 წლის 26 თებერვლის #2 ბრძანების მე-10 მუხლის პირველი პუნქტის ბ) ქვეპუნქტის შესაბამისად წინასწარი ანგარიშსწორების შემთხვევაში, მიმწოდებელი შემსყიდველ ორგანიზაციას წარუდგენს წინასწარ გადასახდელი თანხის ნახევარი ოდენობის გარანტიას, ხელშეკრულებით გათვალისწინებული პირობების შესაბამისად.

***რეზიდენტი მიმწოდებლის მიერ საავანსო-საბანკო გარანტია წარმოდგენილი უნდა იყოს, საქართველოს კანონმდებლობის შესაბამისად ლიცენზირებული დაწესებულებიდან შემდეგი ფორმის დაცვით: დაბეჭდილი გარანტიის გამცემი დაწესებულების ტიტულიან ფურცელზე (ბლანკი), ხელმოწერილი და/ან ბეჭედდასმული;

3.4 ავანსად გაცემული თანხა ჩაითვლება პროპორციულად საბოლოო ანგარიშსწორებისას.

3.5 ანგარიშსწორება განხორციელდება ლარებში უნაღდო ანგარიშსწორების ფორმით გადახდის დღეს საქართველოს ეროვნული ბანკის მიერ დაფიქსირებული ოფიციალური გაცვლითი კურსის მიხედვით აშშ დოლართან მიმართებაში

3.6 მიღება-ჩაბარების აქტის გაფორმებიდან ანგარიშსწორებისათვის განსაზღვრული ვადის დადგომამდე საქონელზე(თანმდევი მომსახურებით) აღმოჩენილი ხარვეზის ან/და ნაკლის არსებობის შემთხვევაში, ,,მიმწოდებელი" ვალდებულია ,,შემსყიდველის" წერილობითი შეტყობინების მიღებისთანავე გონივრულ ვადაში, მაგრამ არაუმეტეს 30 (ოცდაათი) კალენდარული დღის განმავლობაში, საკუთარი ხარჯებით გამოასწოროს აღმოჩენილი ნაკლოვანება ან წუნდებული საქონელი შეცვალოს ახლით. წინააღმდეგ შემთხვევაში აღნიშნული დააყოვნებს ანგარიშსწორების პროცესს იმ ვადით, სანამ მიმწოდებლის მიერ სრულად და ჯეროვნად არ შესრულდება ამ მუხლით განსაზღვრული ვალდებულება;

IV. მხარეთა უფლება-მოვალეობები

4.1. "მიმწოდებელი" მოვალეა გადასცეს "შემსყიდველს" საქონელი (თანმდევი მომსახურებით) (ექსპლუატაციაში არ მყოფი) ხელშეკრულების გაფორმებიდან არაუმეტეს 80 (ოთხმოცი) კალენდარული დღეში წინამდებარე

ხელშეკრულების ფასების ცხრილის (დანართი #1) მიხედვით შემდეგ მისამართზე: სს ,, სსე"-ს სათაო ოფისი, თბილისი, ბარათაშვილის ქუჩა #2 (ტრანსპორტირების ხარჯების გათვალისწინებით).

საქონლის (თანმდევი მომსახურებით) მიწოდება უნდა განხორციელდეს სამუშაო საათებში (ორშაბათიდან პარასკევის ჩათვლით, 09:00 - 18:00 სთ., ოფიციალური უქმე დღეების გარდა).

4.2 საქონლის (თანმდევი მომსახურებით) მოწოდება უნდა განხორციელდეს წინამდებარე ხელშეკრულების დანართი#1–ის (ფასების ცხრილი) და დანართი#2–ის (საქონლის ტექნიკური სპეციფიკაცია) შესაბამისად.

4.3. "შემსყიდველი" მოვალეა:

4.3.1 ხელშეკრულებით გათვალისწინებული პირობების თანახმად გადაიხადოს მიწოდებული საქონლის (თანმდევი მომსახურებით) ღირებულება;

4.3.2 შეამოწმოს საქონლის (თანმდევი მომსახურებით) მდგომარეობა ვარგისიანობაზე;

4.3.3. წერილობით შეატყობინოს "მიმწოდებელს" მიღების ან ექსპლუატაციის დროს საქონელზე შემჩნეული ნაკლის აღმოჩენისთანავე.

V. გარანტია

5.1. "მიმწოდებელი" იძლევა გარანტიას, რომ მიწოდებული საქონელი (თანმდევი მომსახურებით) მისი ექსპლუატაციის ნორმების დაცვის შემთხვევაში, არ გამოავლენს დეფექტებს.

5.2. გადაწყვეტილების ყველა კომპონენტზე ვრცელდება მწარმოებლის 1 (ერთი) წლიანი გარანტია და მხარდაჭერა. საგარანტიო პირობების შესრულებაზე პასუხისმგებლობა ეკისრება უშუალოდ ,,მიმწოდებელს". გარანტია და მხარდაჭერა ვრცელდება პირდაპირ მწარმოებელ კომპანიასთან კომუნიკაციით.

5.3. საგარანტიო ვადის განმავლობაში თუ გამოვლინდება რაიმე ხარვეზი ან შეუსაბამობა, "მიმწოდებელი" ვალდებულია თავისი ხარჯებით გამოასწოროს ხარვეზი "შემსყიდველის" წერილობითი შეტყობინების მიღებიდან 30 (ოცდაათი) კალენდარული დღის განმავლობაში, თუ ეს შეუძლებელია "მიმწოდებელმა" "შემსყიდველის" წერილობითი შეტყობინების მიღებიდან 80 (ოთხმოცი) კალენდარული დღის განმავლობაში უნდა შეცვალოს საქონელი (თანმდევი მომსახურებით) .

VI. ხელშეკრულების შესრულების საგარანტიო უზრუნველყოფა

6.1 "შემსყიდველის" მხრიდან ხელშეკრულების გარანტია ხელშეკრულების შესრულების საგარანტიო უზრუნველყოფა, საბანკო გარანტია, ხელშეკრულების ღირებულების 1%, რომელიც წარმოდგენილია ,,მიმწოდებლის" მიერ გამოყენებული იქნება შემდეგ შემთხვევებში თუ:

ა) "მიმწოდებლის" მხრიდან საქონლის (თანმდევი მომსახურებით) მოწოდების ვადა ირღვევა 30 (ოცდაათი) კალენდარულ დღეზე მეტი ხნის განმავლობაში.

ბ) "მიმწოდებლის" მიერ მოწოდებული საქონელი (თანმდევი მომსახურებით) არ შეესაბამება წინამდებარე ხელშეკრულებით განსაზღვრულ მოთხოვნებს.

6.2 წინამდებარე ხელშეკრულების 6.1 პუნქტით გათვალისწინებულ შემთხვევებში "შემსყიდველი" საბანკო გარანტიის საფუძველზე უპირობოდ და შეუქცევადად იღებს მთელ გარანტირებულ თანხას (ხელშეკრულების ღირებულების 1%).

6.3 "შემსყიდველის" მხრიდან ხელშეკრულების უზრუნველყოფის გარანტიის გამოყენება არ ათავისუფლებს "მიმწოდებელს" წინამდებარე ხელშეკრულების მე-VII მუხლით განსაზღვრული ვალდებულებებისაგან.

VII. მხარეთა პასუხისმგებლობა

7.1 ,,მიმწოდებლის" მიზეზით საქონლის (თანმდევი მომსახურებით) დაგვიანებით, არასრულად, ხარვეზით ან საერთოდ არ მიწოდების შემთხვევაში, ,,მიმწოდებელი" მოვალეა გადაიხადოს პირგასამტეხლო მოუწოდებელი საქონლის (თანმდევი მომსახურებით) ღირებულების 0,1%-ის ოდენობით, ყოველ ვადა გადაცილებულ დღეზე, ხარისხიანი საქონლის (თანმდევი მომსახურებით) სრულად მიწოდების დღემდე ან ხელშეკრულების შეწყვეტის დღემდე, რომელი ვადაც უფრო ადრე დადგება.

7.2 ამ ხელშეკრულების 7.1 პუნქტით გათვალისწინებული პირგასამტეხლო "მიმწოდებელს" გადასახდელად დაერიცხება აგრეთვე იმ შემთხვევაში, თუ მიმწოდებელი არ გამოასწორებს საგარანტიო პერიოდის განმავლობაში გამოვლენილ ხარვეზს ან არ შეცვლის საქონელს ამ ხელშეკრულებით საგარანტიო პერიოდში გამოვლენილი ხარვეზის გამოსწორებისთვის/საქონლის (თანმდევი მომსახურებით) შეცვლისთვის დადგენილ ვადებში - შესატყვისი ვადის გასვლიდან ხარვეზის გამოსწორების/საქონლის (თანმდევი მომსახურებით) შეცვლის დღემდე ან ხელშეკრულების შეწყვეტის დღემდე, რომელი ვადაც უფრო ადრე დადგება.

7.3 „შემსყიდველის" მიერ ხელშეკრულებით გათვალისწინებული საქონლის (თანმდევი მომსახურებით) ღირებულების ვადაგადაცილებით (არადროულად) გადახდის შემთხვევაში, ,,მიმწოდებლი" უფლებამოსილია მოსთხოვოს ,,შემსყიდველს" პირგასამტეხლოს გადახდა გადაუხდელი თანხის 0.1% ოდენობით ყოველ ვადა გადაცილებულ დღეზე წინამდებარე ხელშეკრულების შეწყვეტამდე, ან თანხის სრულად გადახდამდე, რომელი ვადაც უფრო ადრე დადგება.

7.4 ხელშეკრულებით გათვალისწინებული ვალდებულებების ცალმხრივად შეუსრულებლობისათვის მხარეებს ეკისრებათ ვალდებულება აანაზღაურონ მიყენებული ზარალი სრული მოცულობით საქართველოს კანონმდებლობით დადგენილი წესით. ზარალის ანაზღაურება ან მისი მოთხოვნა არ აჩერებს ამ მუხლით გათვალისწინებულ პირგასამტეხლოს დარიცხვას.

7.5 ,,შემსყიდველი“ უფლებამოსილია ფაქტიურად მიწოდებული საქონლის (თანმდევი მომსახურებით) ღირებულების ანაზღაურებისას გამოქვითოს (შეამციროს ანაზღაურება) ამ მუხლით გათვალისწინებული და “მიმწოდებელზე” დარიცხული პირგასამტეხლოს თანხა ,,მიმწოდებლისათვის“ გადასახდელი თანხის ოდენობიდან. აღნიშნული გამოქვითვა არ შეიძლება გახდეს ,,მიმწოდებლის“ მხრიდან ,,შემსყიდველისათვის“ 7.3 პუნქტით გათვალიწინებული პირგასამტეხლოს დარიცხვის საფუძველი.

VIII. ხელშეკრულების შესრულების კონტროლი

8.1 ,,შემსყიდველს“ ან მის წარმომადგენელს უფლება აქვს ხელშეკრულების შესრულების ნებისმიერ ეტაპზე განახორციელოს კონტროლი ,,მიმწოდებლის“ მიერ ნაკისრი ვალდებულებების შესრულებაზე.

8.2 “მიმწოდებელი” ვალდებულია საკუთარი ხარჯებით უზრუნველყოს კონტროლის შედეგად გამოვლენილი ყველა დეფექტის ან ნაკლის აღმოფხვრა.

8.3 ,,შემსყიდველის“ მხრიდან ხელშეკრულების შესრულებაზე კონტროლს ახორციელებს სს ,,საქართველოს სახელმწიფო ელექტროსისტემის“ ინფორმაციული უზრუნველყოფის დეპარტამენტის უფროსი - დავით ნამჩევაძე და ინფორმაციული უზრუნველყოფის დეპარტამენტის უფროსი ინჟინერი - გიორგი თანდაშვილი

8.4 კონტროლი განხორციელდება მიწოდებული საქონლის (თანმდევი მომსახურებით) ხარისხისა და მიწოდების ვადების შესაბამისობით ხელშეკრულების პირობებთან.

IX. ფორს-მაჟორი

9.1 ხელშეკრულების პირობების ან რომელიმე მათგანის მოქმედების შეჩერება ფორს-მაჟორული გარემოებების დადგომის გამო არ იქნება განხილული როგორც ხელშეკრულების პირობების შეუსრულებლობა ან დარღვევა და არ გამოიწვევს საჯარიმო სანქციების გამოყენებას.

9.2 ამ მუხლის მიზნებისათვის ,,ფორს-მაჟორი” ნიშნავს მხარეებისათვის გადაულახავ და მათი კონტროლისაგან დამოუკიდებელ გარემოებებს, რომლებიც არ არიან დაკავშირებული მათ შეცდომებსა და დაუდევრობასთან და რომლებსაც გააჩნიათ წინასწარ გაუთვალისწინებელი ხასიათი. ასეთი გარემოება შეიძლება გამოწვეული იქნას ომით ან სტიქიური მოვლენებით, ეპიდემიით, კარანტინით, ემბარგოს დაწესებით და სხვა. ფორს–მაჟორის არსებობის საკმარის დამადასტურებელ ცნობად მხარეები განიხილავენ შესაბამისი ქვეყნის სავაჭრო–სამრეწველო პალატის მიერ გაცემულ სათანადო ცნობას.

9.3 ფორს-მაჟორული გარემოებების დადგომის შემთხვევაში ხელშეკრულების დამდებმა მხარემ, რომლისთვისაც შეუძლებელი ხდება ნაკისრი ვალდებულებების შესრულება, დაუყოვნებლივ უნდა გაუგზავნოს მეორე მხარეს წერილობითი შეტყობინება ასეთი გარემოებების და მათი გამომწვევი მიზეზების შესახებ. თუ შეტყობინების გამგზავნი მხარე არ მიიღებს მეორე მხარისაგან წერილობით პასუხს, იგი თავისი შეხედულებისამებრ, მიზანშეწონილობისა და შესაძლებლობისდა მიხედვით აგრძელებს ხელშეკრულებით ნაკისრი ვალდებულებების შესრულებას და ცდილობს გამონახოს ვალდებულებების შესრულების ისეთი ალტერნატიული ხერხები, რომლებიც დამოუკიდებელნი იქნებიან ფორს-მაჟორული გარემოებების ზეგავლენისაგან.

X. ურთიერთობა მხარეებს შორის

10.1 ნებისმიერი ოფიციალური ურთიერთობა ხელშეკრულების დამდებ მხარეებს შორის უნდა ატარებდეს წერილობით ფორმას. წერილობითი შეტყობინება, რომელსაც ერთი მხარე ხელშეკრულების შესაბამისად უგზავნის მეორე მხარეს, ხორციელდება საფოსტო გზავნილის ან ელექტრონული კომუნიკაციის გზით ხელმძღვანელობაზე ან /და წარმომადგენლობაზე უფლებამოსილი პირის ან ამ კონტრაქტის ფარგლებში უფლებამოსილი საკონტაქტო პირების (ელექტრონული კომუნიკაციის შემთხვევაში) მიერ. ოპერატილი კავშირის დამყარების მიზნით დასაშვებია შეტყობინების მეორე მხარისათვის მიწოდება ელ. ფოსტით (წერილის სკანირებილი ვარიანტი) ან ფაქსის გაგზავნის გზით, შემდგომში ორიგინალის მიწოდების პირობით.

10.2 შეტყობინება შედის ძალაში ადრესატის მიერ მისი მიღების დღეს ან შეტყობინების ძალაში შესვლის დადგენილ დღეს, იმის მიხედვით, თუ ამ თარიღებიდან რომელი უფრო გვიან დგება.

10.3 ამ მუხლის პირველი პუნქტის მიზნებისთვის ელექტრონული კომუნიკაციის წარმოების პროცესში პასუხისმგებელი პირის დანიშვნა, საკონტაქტო საკითხების მითითებით ხორციელდება მხარის მიერ წერილობითი შეტყობინების საფუძველზე.

XI.ხელშეკრულების პირობების შეცვლა და/ან ვადამდე მოშლა

11.1 ამ ხელშეკრულებაში ნებისმიერი ცვლილება და/ან დამატება შეიძლება შეტანილი იქნეს მხარეთა წერილობითი შეთანხმების საფუძველზე.

11.2 შესყიდვის შესახებ ხელშეკრულების პირობების შეცვლა დაუშვებელია, თუ ამ ცვლილების შედეგად იზრდება ხელშეკრულების საერთო ღირებულება ან უარესდება ხელშეკრულების პირობები შემსყიდველი ორგანიზაციისათვის, გარდა საქართველოს სამოქალაქო კოდექსის 398-ე მუხლით გათვალისწინებული შემთხვევისა, ამასთან, ასეთ შემთხვევაშიც დაუშვებელია ხელშეკრულების ჯამური ღირებულების 10%–ზე მეტი ოდენობით გაზრდა.

11.3. ხელშეკრულება შეიძლება ვადამდე მოიშალოს:

11.3.1. მხარეთა შეთანხმებით;

11.3.2. ერთ-ერთი მხარის განცხადებით მეორე მხარის მიერ ხელშეკრულებით გათვალისწინებული პირობების არსებითად დარღვევის შემთხვევაში;

11.4 ,,შემსყიდველს“ შეუძლია ხელშეკრულება ვადამდე შეწყვიტოს:

11.4.1. თუ “შემსყიდველისათვის” ცნობილი გახდა, რომ მისგან დამოუკიდებელი მიზეზების გამო იგი ვერ უზრუნველყოფს ხელშეკრულებით ნაკისრი ვალდებულებების შესრულებას;

11.4.2. ,,მიმწოდებლის“ გაკოტრების შემთხვევაში;

11.4.3 თუ მისთვის ცნობილი გახდება, რომ “მიმწოდებლის” მიერ მოწოდებული ინფორმაცია ყალბი აღმოჩნდება, რაც წარმოადგენს, ,,შემსყიდველის“ მხრიდან ნდობის დაკარგვის საფუძველს.

11.4.4. საქართველოს კანონმდებლობით გათვალისწინებულ სხვა შემთხვევებში.

11.5 ამ მუხლის 11.4 პუნქტში მითითებულ შემთხვევებში “შემსყიდველი” ვალდებულია აუნაზღაუროს “მიმწოდებელს” ფაქტიურად მიწოდებული საქონლის (თანმდევი მომსახურებით) ღირებულება.

XII. ხელშეკრულების შესრულების შეფერხება

12.1 თუ ხელშეკრულების შესრულების პროცესში მხარეები წააწყდებიან რაიმე ხელშემშლელ გარემოებებს, რომელთა გამო ფერხდება ხელშეკრულების პირობების შესრულება, ამ მხარემ დაუყოვნებლივ უნდა გაუგზავნოს მეორე მხარეს წერილობითი შეტყობინება შეფერხების ფაქტის, მისი შესაძლო ხანგრძლივობის და გამომწვევი მიზეზების შესახებ. შეტყობინების მიმღებმა მხარემ რაც შეიძლება მოკლე დროში უნდა აცნობოს მეორე მხარეს თავისი გადაწყვეტილება, მიღებული აღნიშნულ გარემოებებთან დაკავშირებით.

12.2 იმ შემთხვევაში, თუ ხელშეკრულების პირობების შესრულების შეფერხების გამო მხარეები შეთანხმდებიან ხელშეკრულების პირობების შესრულების ვადის გაგრძელების თაობაზე, ეს გადაწყვეტილება უნდა გაფორმდეს ხელშეკრულებაში ცვლილების შეტანის გზით.

XIII. დავათა განხილვა

13.1 ხელშეკრულების დამდები მხარეები თანხმდებიან მასზედ, რომ ყველა ღონეს იხმარენ, რათა მოლაპარაკებების მეშვეობით, შეთანხმებით მოაგვარონ ნებისმიერი უთანხმოება და დავა, წარმოქმნილი მათ შორის ხელშეკრულების ან მასთან დაკავშირებული საკითხების ირგვლივ.

13.2 თუ ასეთი მოლაპარაკების დაწყებიდან 30 (ოცდაათი) კალენდარული დღის განმავლობაში მხარეები ვერ შესძლებენ სადაო საკითხების შეთანხმებას, ნებისმიერ მხრეს დავის გადაწყვეტის მიზნით შეუძლია დადგენილი წესით მიმართოს საქართველოს სასამართლოს. დავის განხილვა მოხდება საქართველოს კანონმდებლობის შესაბამისად.

XIV. შესყიდვის ობიექტის მიღება-ჩაბარების წესი

14.1 მიღება -ჩაბარების აქტები ფორმდება ფაქტიურად მოწოდებული საქონლის (თანმდევი მომსახურებით) მიხედვით.

14.2 საქონლის (თანმდევი მომსახურებით) მოწოდებისას “შემსყიდველის” მიერ წინამდებარე ხელშეკრულების 8.3 ქვეპუნქტით განსაზღვრული პირი ამოწმებს მოწოდებული საქონლის (თანმდევი მომსახურებით) შესაბამისობას წინამდებარე ხელშეკრულების პირობებთან, ხარვეზების (წუნდების) არ არსებობის შემთხვევაში ფორმდება მიღება-ჩაბარების აქტი ფაქტიურად მიღებული საქონლის (თანმდევი მომსახურებით) მიხედვით ,,შემსყიდველსა“ და ,,მიმწოდებელს“ შორის.

14.3 საქონელი (თანმდევი მომსახურებით) მიღებულად ჩაითვლება მხარეთა შორის მიღება-ჩაბარების აქტის გაფორმებისთანავე. მიღება-ჩაბარების გაფორმების შემდგომ პასუხისგებლობა საქონელზე გადადის შემსყიდველზე.

14.4 ,,შემსყიდველის“ მხრიდან მიღება-ჩაბარების აქტზე ხელმომწერ პირად განისაზღვროს - სს ,,სსე“-ს შესაბამისი უფლებამოსული პირი.

XV. ხელშეკრულების მოქმედების ვადები

15.1. ხელშეკრულება ძალაში შედის მხარეთა მიერ ხელმოწერისთანავე.
15.2. ხელშეკრულების მოქმედების ვადა ამოწურულად ჩაითვლება აღნიშნული პირობების შესრულებისთანავე, მაგრამ არაუგვიანეს **2020 წლის 31 მარტის ჩათვლით,** ხოლო საგარანტიო ვალდებულებების ნაწილში საგარანტიო ვადის ბოლომდე.

XVI. ხელშეკრულების სხვა პირობები

16.1 ხელშეკრულება შედგენილია ქართულ ენაზე ან/და ინგლისურ ენაზე ორ ეგზემპლარად და ყოველ მათგანს გააჩნია თანაბარი იურიდიული ძალა.
16.2 ამ ხელშეკრულებით გაუთვალისწინებელ შემთხვევებში, მხარეები მოქმედებენ საქართველოში მოქმედი კანონმდებლობის თანახმად.
16.3 წინამდებარე ხელშეკრულებით გათვალისწინებული პირობები შესასრულებლად სავალდებულოა მხარეთათვის და მათი შესაბამისი სამართალმემკვდრეებისა და უფლებამონაცვლეთათვის. დაუშვებელია წინამდებარე ხელშეკრულებით გათვალისწინებული ვალდებულებების გადაცემა სხვა მხარისათვის მეორე მხარის წინასწარი წერილობითი თანხმობის გარეშე.
16.4 წინამდებარე ხელშეკრულებით გათვალისწინებული პირობები, პროგრამის დეტალები, ხელშეკრულების ფარგლებში „მომწოდებლისთვის" „შემსყიდველის" მიერ მიწოდებული ან/და თანდართული მომსახურების გაწევის დროს გაცვლილი ნებისმიერი ინფორმაცია წარმოადგენს
კონფედენციალურ ინფორმაციას და არ უნდა მოხდეს მათი გამჟღავნება სხვა მხარისათვის, გარდა კანონმდებლობით გათვალისწინებული შემთხვევებისა.
16.5 წინამდებარე ხელშეკრულება დაიდო სახელმწიფო შესყიდვის შესახებ საქართველოს კანონის მე-3 მუხლის პირველი პუნქტის ჟ) ქვეპუნქტის შესაბამისად.

XVII. კონფიდენციალურობა და გაუმჟღავნებლობა

17.1 მხარეები აცნობიერებენ, რომ სს „საქართველოს სახელმწიფო ელექტროსისტემაში" დანერგილია ინფორმაციული უსაფრთხოების მართვის სისტემა ISO/IEC 27001 მიხედვით და შესაბამისად, შემდგომ ურთიერთობებში ითვალისწინებენ „სს „საქართველოს სახელმწიფო ელექტროსისტემის" კონფიდენციალურობისა და გაუმჟღავნებლობის პირობებს", რომელიც გამოქვეყნებულია ვებ-გვერდზე www.gse.com.ge (ჩვენს შესახებ/შესყიდვები/კონტრაქტის პირობები).

XVIII. თანმდევი მომსახურება

18.1 ,,თანმდევი მომსახურება" გულისხმობს მოწოდებული საქონლის ინსტალაციას

XIX . მხარეთა რეკვიზიტები

"შემსყიდველი":
სს ,,საქართველოს სახელმწიფო ელექტროსისტემა"

ქ. თბილისი, ბარათაშვილის ქ. №2
საიდ. კოდი: 204995176
სს „თიბისი ბანკი"
ცენტრალური ფილიალი
ბანკის კოდი: TBCBGE22
ანგარიშის № GE02TB0600000010246763 6

დავით ვარდიაშვილი
მმართველთა საბჭოს წევრი

"მიმწოდებელი":
შპს „იუჯითი"

ქ.თბილისი. ჭავჭავაძის 17ა
საიდ. კოდი: 204892964
სს „საქართველოს ბანკი"
ბანკის კოდი: BAGAGE22
ა/ა: GE88BG0000000261644601
სს „თიბისი ბანკი"
ბანკის კოდი: TBCBGE22
ა/ა: GE05 TB0600000005467291

ერმილე სულაძე
გენერალური დირექტორი

დანართი # 1

ფასების ცხრილი:

	საქონლის (თანმდევი მომსახურებით) დასახელება	მწარმოებელი კომპანია/ წარმოშობის ქვეყანა	რაოდენობა	ერთეულის ფასი დღგ-ს ჩათვლით (აშშ დოლარი)	ჯამური ფასი დღგ-ს ჩათვლით (აშშ დოლარი)
1	2	2	3	5	6
1	ინფორმაციული უსაფრთხოების სისტემა	McAfee / ირლანდია	1	304894,16	304894,16
2	თანმდევი მომსახურება	x	x	x	4006,38
მთლიანი ფასი დღგ-ს ჩათვლით (აშშ დოლარი)					308 900,54

"შემსყიდველი":

სს ,,საქართველოს სახელმწიფო ელექტრონული სისტემა"

დავით ვარდიაშვილი
მმართველობის საბჭოს წევრი

"მიმწოდებელი":

შპს ,,იუჯითი"

ერმილე სულაძე
გენერალური დირექტორი

დანართი # 2

საქონლის (თანმდევი მომსახურებით) ტექნიკური სპეციფიკაცია

საქონლის (თანმდევი მომსახურებით) ტექნიკური სპეციფიკაცია	
1. მოთხოვნები SIEM გადაწყვეტილებისა და მასში შემავალი სისტემების მიმართ	
შემოთავაზებული SIEM გადაწყვეტილების ყველა კომპონენტის, ფუნქციონალის მართვა ხორციელდებება ცენტრალიზებულად, ერთიანი Web ინტერფეისის საშუალებით;	
SIEM გადაწყვეტილებას აქვს კომპონენტებს შორის კომუნიკაციის შიფრაციის შესაძლებლობა;	
SIEM-ის გადაწყვეტილებაში შესაძლებელია საინფორმაციო რესურსების (წყაროების) ხდომილებების ჟურნალირება, დამუშავება, კორელაცია და ანალიტიკა;	
გადაწყვეტილებას აქვს API მონაცემთა ბაზაში განთავსებული ინფორმაციის გაზიარებისათვის;	
SIEM გადაწყვეტილება ინტეგრირდება MS AD-ს მომხმარებლების აუთენტიფიკაციის უზრუნველყოფისათვის;	
SIEM გადაწყვეტილებას უნდა შეეძლოს ინტეგრაცია:	SIEM გადაწყვეტილებას შეუძლია IPS / IDS-თან ინტეგრაცია;
	SIEM გადაწყვეტილებას შეუძლია საწარმოს SCADA-ს ქსელში არსებულ მოწყობილობებსა და ინფორმაციულ სისტემებთან ინტეგრაცია;
	SIEM გადაწყვეტილებას აქვს საწარმოს ICON-ის ქსელში არსებულ მოწყობილობებსა და ინფორმაციულ სისტემებთან ინტეგრაციის შესაძლებლობა;
	SIEM გადაწყვეტილებას შეუძლია საწარმოს IT ქსელში არსებულ მოწყობილობებსა და ინფორმაციულ სისტემებთან ინტეგრაცია
SIEM გადაწყვეტილებას აქვს ცალკეული კომპონენტების მუშაობის უზრუნველყოფის საშუალება ერთ-ერთი კომპონენტის მწყობრიდან გამოსვლის შემთხვევაშიც (მაგალითად, ცენტრალური კონსოლის მწყობრიდან გამოსვლის შემთხვევაში ხდომილებების მიმღები სისტემა აგრძელებდეს ფუნქციონირებას);	
SIEM გადაწყვეტილებას აქვს კონფიგურაციის ავტომატიზებული რეზერვირების (Backup) და აღდგენის (Recovery) შესაძლებლობა მომხმარებლის გრაფიკული კონსოლიდან;	
SIEM გადაწყვეტილებას აქვს თავისი მდგომარეობის ანალიზის შესაძლებლობა და მომხმარებლის შეტყობინების საშუალება პრობლემის წარმოქმნის შემთხვევაში;	
SIEM გადაწყვეტილებას უნდა შეეძლოს ნაკადების (Flows) წაკითხვა და დამუშავება:	SIEM გადაწყვეტილებას შეეძლია ნაკადების (Flows) წაკითხვა და დამუშავება, აქვს NetFlow პროტოკოლის პროტოკოლების მხარდაჭერა
	SIEM გადაწყვეტილებას აქვს ასევე აქვს ქსელის ნაკადების წაკითხვის და ანალიზის შესაძლებლობა L7 დონეზე (ქსელის OSI მოდელის მიხედვით);
	SIEM გადაწყვეტილებას შეუძლია VMware-ს ვირტუალური ინფრასტრუქტურის ნაკადების წაკითხვისა და დამუშავების შესაძლებლობა.

SIEM გადაწყვეტილებას შეუძლია ქსელის ტრაფიკის პროფილირება L7 დონეზე (ქსელის OSI მოდელის მიხედვით);	
SIEM გადაწყვეტილებას აქვს შემომავალი ხდომილებების წამში - 20 000 ხდომილება / წამში დამუშავების შესაძლებლობა.	
პიკური დატვირთვის დროს თუ ხდომილებების და/ან ნაკადების რაოდენობამ წამში გადააჭარბა ზემოთ მოთხოვნილ რაოდენობას, SIEM გადაწყვეტილება შეატყობინებს სისტემის ადმინისტრატორს და მონაცემების დაუკარგავად გააგრძელოს ფუნქციონირება;	
SIEM გადაწყვეტილებას აქვს ხდომილებების ჟურნალების შეგროვების და არქივაციის შესაძლებლობა. ჟურნალების შენახვა შესაძლებელია როგორც online, ისე offline რეჟიმში;	
SIEM გადაწყვეტილებას შეუძლია ჟურნალების შენახვა გარე მატარებლებზე;	
SIEM გადაწყვეტილებას აქვს აგენტების გარეშე ხდომილებების შეგროვების შესაძლებლობა, იქ სადაც ეს შესაძლებელია;	
SIEM გადაწყვეტილებას შეუძლია ხდომილებების სრული ინფორმაციაზე წვდომის უზრუნველყოფა, ხდომილებების არსებობის პერიოდის განმავლობაში;	
SIEM გადაწყვეტილებას შეუძლია ხდომილებების ინფორმაციის შენახვა, როგორც საწყის ფორმაში, ასევე ნორმალიზებული სახით, შემდგომი ანალიზისათვის;	
SIEM გადაწყვეტილებას ავქს ხდომილებების ანალიზის შესაძლებლობა რეალურ რეჟიმში;	
SIEM გადაწყვეტილებას აქვს ხდომილებების ანალიზის შესაძლებლობა კონკრეტული პერიოდის განმავლობაში, რომელიც მითითებული იქნება ანალიტიკოსის/ადმინისტრატორის მიერ;	
SIEM გადაწყვეტილებაში რეალიზებულია რეპორტების გენერაციის შესაძლებლობა. სისტემაში არსებობს წინასწარ განსაზღვრული რეპორტების ნიმუშები (შაბლონები). ასევე სისტემაში არის საკუთარი რეპორტების გენერაციის შესაძლებლობა;	
SIEM გადაწყვეტილებაში რეალიზებულია, გარკვეული დროს პერიოდში, რეპორტების ავტომატიზებული გენერაციის შესაძლებლობა;	
SIEM სისტემაში არსებობს ხდომილებების კორელაციის გამზადებული წესები (წესების ჩამონათვალი);	
SIEM გადაწყვეტილებას გააჩნია ქსელური ტრაფიკის და პროცესების ანომალური ქმედებების აღმოჩენის და ანალიზის შესაძლებლობა;	
SIEM გადაწყვეტილებაში რეალიზებულია სერვისების ამოცნობის მექანიზმი;	
SIEM გადაწყვეტილებას შეუძლია ქსელურ ტრაფიკში განასხვავოს და პროფილირება გაუწიოს სხვა და სხვა აპლიკაციებს, არა მარტო ცნობილი TCP პორტების საშუალებით;	
SIEM გადაწყვეტილებას შეუძლია ქსელურ ტრაფიკში ნაკადების დეტექტირება და იდენტიფიცირება გეოგრაფიული რეგიონების მიხედვით რეალურ დროში;	
SIEM გადაწყვეტილებაში რეალიზებული უნდა იყოს IP	SIEM გადაწყვეტილებაში რეალიზებულია IP Reputation მექანიზმები. სისტემას ავტომატიზებულად შეეძლია შეერთებების გამოვლენა BotNet ქსელებთან;

Reputation მექანიზმები. სისტემას ავტომატიზებულად უნდა შეეძლოს შეერთებების გამოვლენა:	SIEM გადაწყვეტილებაში რეალიზებულია IP Reputation მექანიზმები. სისტემას ავტომატიზებულად შეეძლია შეერთებების გამოვლენა Mailware რესურსებთან;
	SIEM გადაწყვეტილებაში რეალიზებულია IP Reputation მექანიზმები. სისტემას ავტომატიზებულად შეეძლია შეერთებების გამოვლენა Spam საიტებთან.
SIEM ინტერფეისში შესაძლებელია პირდაპირ ამ ტექნიკური დავალების მე-2 პუნქტში მოცემული „სამუშაო სადგურების ცენტრალური მართვის კონსოლის" გაშვება და სამუშაო სადგურებზე (მათ შორის, მომხმარებელთა კომპიუტერები და სერვერები) დამატებითი დეტალური ინფორმაციის ამავე ინტერფეისიდან ნახვა;	
SIEM გადაწყვეტილებას შეეძლია საფრთხეებისგან დაცვის („სენდბოქსის") სისტემის ინტეგრაცია. ინტეგრაციის შედეგად, საფრთხეებისგან დაცვის („სენდბოქსის") გადაწყვეტილება აგზავნის საფრთხის შემცველი ინდიკატორების (IOCs) დეტალურ ინფორმაციას SIEM-ში;	
გადაწყვეტას აქვს საკუთარი რეპუტაციის ლოკალური სისტემა, რომელსაც შეუძლია ინტეგრაცია SIEM, სენდბოქსის სისტემასა და სამუშაო სადგურების დაცვის მართვის სისტემებთან. შედეგად, აღნიშული ყველა სისტემა იღებს მუდმივად განახლებულ ინფორმაციას ლოკალურად ქსელში არსებული საფრთხეების შესახებ ინტერნეტთან წვდომის არ ქონის შემთხვევაშიც;	
SIEM გადაწყვეტილებას ცენტრალურ მართვის კონსოლში შეუძლია სისტემების ავტომატური მარკირება (იგულისხმება სისტემები, სადაც დიდი ალბათობაა შეტევის განხორციელების ან უკვე დაგროვდა კრიტიკული რაოდენობა საფრთხის შემცველი მოვლენების) - შედეგად, სამუშაო სადგურების ცენტრალურ მართვის კონსოლში შესაძლებელია წინასწარ გაწერილი პოლიტიკების ავტომატურად გააქტიურება, რის საფუძველზეც შესაძლებელია საფრთხეების რეალურ დროში პრევენცია;	
1.1 მართვის ძირითადი სისტემა	
მართვის ძირითად სისტემაში ინტეგრირდებება SIEM გადაწყვეტილებაში შემავალი ყველა სისტემა;	
გადაწყვეტილების ინტეგრაციის შემდეგ, სამუშაო სადგურების ცენტრალური მართვის კონსოლისთვის შესაძლებელია უსაფრთხოების რეაგირების ქმედებების შექმნა;	
მართვის ძირითად სისტემას შეუძლია რეალურ დროში სისტემების, ქსელების, მონაცემთა ბაზებისა და აპლიკაციების ქმედების ჩვენება, ხდომილებების შეგროვება, დამუშავება;	
მართვის ძირითად სისტემას გააჩნია ინტერაქტიული და რედაქტირებადი ხელსაწყოთა პანელი, რომლის გამოყენებაც შესაძლებელია ინციდენტის გამოძიებისას;	
მართვის ძირითად სისტემას გააჩნია ცენტრალიზებული ანალიტიკის ხელსაწყოთა პანელი;	
მართვის ძირითად სისტემას გააჩნია წინასწარ შედგენილი ხელსაწყოთა პანელი;	
მართვის ძირითად სისტემა წარმოადგენდეს აპარატურულ -პროგრამულ (Appliance) გადაწყვეტილებას;	

მინიმალური მოთხოვნები მართვის ძირითად სისტემის აპარატურის მიმართ:	ხდომილებების დამუშავება:	20.000 ხდომილების წამში დამუშავება
	მაქსიმალური ხდომილებების მიღების საშუალება:	70,000 ხდომილების წამში მიღების საშუალება.
	ლოკალური საცავი:	აქვს 32 TB ლოკალური საცავი.
	ქსელური ინტერფეისები:	აქვს 2 x 10Gb პორტი ქსელური ინტერფეისები.
	რაოდენობა	რაოდენობა 1 ცალი

1.2 კორელაციის სისტემა

სისტემას შეუძლია რისკისა და შეტევის აღმოსაჩენად რეალურ რეჟიმში გაანალიზოს შეგროვებული შემთხვევები;
სისტემაში აქვს ფუნქციონალი, რომელიც დააგენერირებს „განგაშს“(Alert) თუ დაფიქსირდა შეტევა მომხმარებლებზე, აპლიკაციებზე, ქსელზე;
სისტემა იძლევა ახალი შეტევის, მოწყვლადობის შემოწმების საშუალებას, ძველ ხდომილებებზე დაყრდნობით;
სისტემას შეუძლია გაჰყვეს ყველა აქტივობას, რომელიც დაკავშირებულია კონკრეტულ ხდომილებასთან და შეიმუშაოს დინამიური რისკის ქულა, რომლის მომატება და კლება დაკავშირებულია რეალური დროში არსებულ აქტივობასთან;
სისტემა იძლევა წესებით კორელაციის საშუალებას; სისტემა იძლევა წესების გარეშე კორელაციის საშუალებას;
სისტემას მოყვება ხდომილებების კორელაციის წინასწარ განსაზღვრული წესები;
სისტემას გააჩნია ხდომილებების კორელაციის წესები შექმნისა და კონფიგურაციის გრაფიკული ინტერფეისი;
სისტემა წარმოადგენს აპარატურულ-პროგრამულ (Appliance) გადაწყვეტილებას.

მინიმალური მოთხოვნები კორელაციის სისტემის აპარატურის მიმართ:	მაქსიმალური ხდომილებების მიღებების საშუალება:	75,000 ხდომილების წამში მიღების შესაძლებლობა.
	ლოკალური საცავი:	აქვს 12 TB ლოკალური საცავი
	ქსელური ინტერფეისები:	აქვს 2 x 10Gb ქსელური ინტერფეისის პორტი
	რაოდენობა:	რაოდენობა 1 ცალი

1.3 ჟურნალების მართვის სისტემა		
ჟურნალების მართვის სისტემა იძლევა წვდომის საშუალებას ე.წ. ერთი ღილაკის დაჭერით, მის მოდულში არსებული ყველა ჟურნალის ჩანაწერის ორიგინალში ნახვის საშუალებას;		
ჟურნალების მართვის სისტემას გააჩნია ჟურნალების შეგროვებისა და შენახვის საჭირო ფუნქციონალი;		
ჟურნალების მართვის სისტემა იძლევა ჟურნალების შენახვის საშუალებას ლოკალურად მოდულში. ჟურნალების მართვის სისტემა იძლევა ჟურნალების შენახვის საშუალებას გარე შესანახ არეაში (storage area);		
ჟურნალების მართვის სისტემა იძლევა მეხსიერების საცავის რამდენიმე აპარატურისგან შედგენის საშუალებას და მონაცემების მიბმას კონკრეტულ მეხსიერების საცავზე;		
სისტემა წარმოადგენს აპარატურულ-პროგრამულ (Appliance) გადაწყვეტილებას;		
მინიმალური მოთხოვნები სისტემის აპარატურის მიმართ:	მაქსიმალური ხდომილებების მიღებების საშუალება:	75,000 ხდომილების წამში მიღების საშუალება
	ლოკალური საცავი:	აქვს 32 TB ლოკალური საცავი.
	ქსელური ინტერფეისები:	აქვს 2 x 10Gb ქსელური ინტერფეისის პორტი
	რაოდენობა:	რაოდენობა 1 ცალი
1.4 აპლიკაციების მონიტორინგი		
აპლიკაციების მონიტორინგის სისტემას გააჩნდეს მოდული, რომელიც შეძლებს ქსელის დონეზე დააფიქსიროს სენსიტიური მონაცემების გადაცემა, ნებისმიერი აპლიკაციის საშუალებით;		
სისტემას გააჩნია მოდული, რომელიც შეძლებს დააფიქსიროს სახიფათო პროგრამული კოდი L7 დონეზე (ქსელის OSI მოდელის მიხედვით);		
სისტემას გააჩნია მოდული, რომელიც დააფიქსირებს არა ავტორიზებულ აპლიკაციის გამოყენებას;		
სისტემას გააჩნია მოდული, რომელიც შეძლებს დააფიქსიროს აპლიკაციის შეტევის წყაროები;		
სისტემას გააჩნია მოდული, რომელიც შეძლებს დააფიქსიროს მომხმარებლის ჩანაწერების (user credentials) ქურდობა და არასწორად გამოყენება.		

სისტემას შეუძლია დააფიქსიროს აპლიკაციაში დამალული მავნე კოდები, ვირუსები, დოკუმენტებში ჩაშენებული გამშვები ფაილები;		
სისტემა წარმოადგენს აპარატურულ (Appliance) გადაწყვეტილებას.		
მინიმალური მოთხოვნები სისტემის აპარატურის მიმართ:	ქსელური ტრაფიკის დამუშავება:	1Gbps ქსელური ტრაფიკის დამუშავების შესაძლებლობა.
	ლოკალური საცავი:	აქვს 4 TB ლოკალური საცავი.
	ქსელური ინტერფეისები:	აქვს 2 x 1Gb ქსელური ინტერფეისის პორტი
	რაოდენობა:	რაოდენობა 1 ცალი
1.5 ხდომილებების მიმღები სისტემა		
სისტემას შეუძლია ხდომილებებისა და ნაკადების (Flows) სხვადასხვა სისტემებიდან მიღება;		
სისტემას გააჩნია ფუნქციონალი დაამუშაოს ხდომილებები და შეინახოს მონაცემთა ბაზაში ინდექსირებული სახით, რათა შესაძლებელი იყოს სწრაფი წვდომა საჭიროების შემთხვევაში;		
სისტემა წარმოადგენდეს აპარატურულ (Appliance) გადაწყვეტილებას.		
მინიმალური მოთხოვნები კორელაციის სისტემის აპარატურის მიმართ:	მაქსიმალური ხდომილებების მიღებების საშუალება წამში:	14000 ხდომილებების მიღებების საშუალება წამში
	ლოკალური საცავი:	აქვს 12TB ლოკალური საცავი.
	ქსელური ინტერფეისები:	აქვს 2 x 10Gb ქსელური ინტერფეისის პორტი
	რაოდენობა:	რაოდენობა 2 ცალი
2. სამუშაო სადგურების ცენტრალური მართვის კონსოლი		
ცენტრალური მართვის კონსოლს შეუძლია მოდულების დაყენება როგორც ავტომატურ, ასევე მექანიკურ რეჟიმში;		
ცენტრალური მართვის კონსოლს შეეძლია განახლებული სისტემების მხარდაჭერა (პროგრამული განახლება, პოლიტიკების სინქრონიზაცია);		
ცენტრალური მართვის კონსოლს შეუძლია დროის რეალურ რეჟიმში სამუშაო სადგურების მდგომარეობის კონტროლი;		

ცენტრალური მართვის კონსოლს შეუძლია სისტემების ავტომატური დახარისხება მათი ტიპებით, აპარატურული რესურსებით და სხვა პარამეტრებით;
ცენტრალური მართვის კონსოლს შეუძლია ინდივიდუალური სისტემების და სისტემათა ჯგუფების დონეზე განსხვავებული პოლიტიკების დანიშვნის შესაძლებლობა;
ცენტრალური მართვის კონსოლს შეუძლია დაცვის მოდულების ინსტალაციის, განახლების და კონტროლის ამოცანების დაგეგმვის ჩაშენებული მექანიზმი;
ცენტრალური მართვის შეუძლია ორგანიზაციის სტრუქტურის, ჯგუფების, ქვეჯგუფების დონეზე ცალკეული დავალებების განსაზღვრა;
ცენტრალური მართვის კონსოლს შეუძლია პოლიტიკების კატალოგების შენახვა, მათი ასლების შექმნა და რეკონფიგურირების შესაძლებლობა სპეციფიურ ჯგუფებზე;
ცენტრალური მართვის კონსოლს შეუძლია განსხვავებული პოლიტიკებისა და განსხვავებული ამოცანების (Task) შედარების შესაძლებლობა;
ცენტრალური მართვის კონსოლს აქვს შესაძლებლობა გამოაჩინოს პოლიტიკის ცვლილებისას რამდენ სისტემაზე მოახდენს გავლენას პოლიტიკის ცვლილება;
ცენტრალური მართვის კონსოლს შეუძლია კონსოლის ოპერატორების ქმედებების აღრიცხვა (აუდიტი);
ცენტრალური მართვის კონსოლს შეუძლია აუთენტიფიკაციისთვის Active Directory-ის ანგარიშების გამოყენების შესაძლებლობა;
ცენტრალური მართვის კონსოლს შეუძლია სამუშაო სადგურებიდან აღრიცხული ხდომილების მიღება და დამუშავება;
ცენტრალური მართვის კონსოლს შეუძლია ინდივიდუალური სამუშაო სადგურების და ჯგუფების დონეზე კავშირის ინტერვალის კონფიგურაციის შესაძლებლობა;
ცენტრალური მართვის კონსოლს შეუძლია ინდივიდუალური სამუშაო სადგურების და ჯგუფების დონეზე კავშირის ინტერვალის კონფიგურაციის შესაძლებლობა;
საფრთხეების სრულყოფილად აღმოჩენისა და სწრაფი რეაგირებისთვის, ამავე მწარმოებლის SIEM გადაწყვეტილებიდან შესაძლებელია სამუშაო სადგურების ცენტრალური მართვის სისტემისთვის უსაფრთხოების ავტომატიზებული რეაგირების ქმედებების შექმნა.
2.1 რეპუტაციის ლოკალური სერვერი
რეპუტაციის ლოკალურ სერვერს შეუძლია დაუკავშირდეს და მოახდინოს ინფორმაციის თანაფარდობა VirusTotal-თან სპეციფიური საფრთხის ნიმუშზე;

რეპუტაციის ლოკალურ სერვერს შეუძლია აფრთხეების შესახებ ინფორმაციის შეტანის შესაძლებლობა მექანიკურ რეჟიმში რეპუტაციის ლოკალურ სერვერზე;	
რეპუტაციის ლოკალურ სერვერს შეუძლია ინფიცირებული სამუშაო სადგურის იზოლირება, შეტევის იდენტიფიცირება ლოკალური რეპუტაციის სერვერისა და მანქანური სწავლების ალგორითმის გაოყენებით. ასევე შესაძლებელია სხვა ქვესისტემების ინფორმირება ორგანიზაციაში არსებული საფრთხეების შესახებ და ხდომილების გაგზავნა SIEM სისტემაში.	
2.2 დაინფიცირებული სისტემების რეაგირების ქვესისტემა	
ქვესისტემამ უზრუნველყოფს სამუშაო სადგურების შემოწმებას დაინფიცირების გამოსავლენად;	
აქტიურ რეაგირებაზე მხარდაჭერილი ოპერაციული სისტემების ჩამონათვალი: Windows ვერსია 7 და ზემოთ;	
მართვის კონსოლის ოპერატორს ქვესისტემა უნდა აძლევდეს შემდეგ შესაძლებლობებს:	მართვის კონსოლის ოპერატორს ქვესისტემა აძლევეს ინფიცირებული სისტემების მარკირების შესაძლებლობებს;
	მართვის კონსოლის ოპერატორს ქვესისტემა აძლევეს სამუშაო სადგურებიდან ინფორმაციის შეგროვების შესაძლებლობას;
	მართვის კონსოლის ოპერატორს ქვესისტემა აძლევეს ინფიცირებული სისტემებისთვის ავტომატიზებული ამოცანების შექმნის შესაძლებლობას.
ქვესისტემა უნდა შეიცავდეს ძებნის შემდეგ კრიტერიუმებს:	ქვესისტემა შეიცავს გაშვებული პროცესების დასახელებებით ძებნის კრიტერიუმს;
	სისტემების IP მისამართებით ძებნის კრიტერიუმს;
	ქსელური პორტების ნომრებით ძებნის კრიტერიუმს;
	პროტოკოლების ტიპებით ძებნის კრიტერიუმს;
	ფაილის სახელებით ძებნის კრიტერიუმს;
	სისტემების დასახელებებით ძებნის კრიტერიუმს;
	დაყენებული განახლებების აღწერილობებით ძებნის კრიტერიუმს;
	მომხმარებელთა ანგარიშების პარამეტრებით ძებნის კრიტერიუმს;
	გაშლილი ინფორმაცია გაშვებულ პროცესებზე (path, command line, inheritance) ძებნის კრიტერიუმს;
ქვესისტემას უნდა გააჩნდეს ავტომატიზებული ქმედების მექანიზმი მავნე კოდის	აქვს მითითებული ფაილის შექმნაზე თვალთვალის შესაძლებლობა; აქვს მითითებული ფაილის წაშლაზე თვალთვალის შესაძლებლობა; აქვს მითითებული ფაილის ცვლილებაზე თვალთვალის შესაძლებლობა;

შეღწევადობის შედეგების აღმოსაფხვრელად (სისტემის რეაბილიტაცია), რომელიც უნდა შეიცავდეს შემდეგ სცენარებს:	დამყარებულ და განყვეტილ ქსელურ შეერთებებზე თვალთვალის სესაძლებლობა;
	ღია პორტებზე თვალთვალის შესაძლებლობა;
	მეხსიერებიდან გაშვებული პროცესების თვალთვალის შესაძლებლობა; მეხსიერებიდან დასრულებული პროცესების თვალთვალის შესაძლებლობა;
	სისტემის გამორთვის შესაძლებლობა; სისტემის გადატვირთვის შესაძლებლობა;
	პროცესების გამორთვის შესაძლებლობა;
	ქსელური შეერთებების დაკეტვის შესაძლებლობა;
	სისტემური სერვისების გაჩერების შესაძლებლობა;
მავნე კოდის არსებობის შედეგების აღმოსაფხვრელად ქვესისტემას გააჩნია ავტომატიზებული ქმედების მექანიზმის ჩაშენებული კონსტრუქტორი გაფართოებული შესაძლებლობებით;	
ლიცენზიების რაოდენობა:	1000 ცალი

2.3 სამუშაო სადგურების დაცვა

სისტემას შეუძლია ფაილებზე მიმართვის დროს (ე.წ. On-Access Scan), წაკითხვისას, ჩაწერისას და მათი დეტალური სკანირება;
სისტემას შეუძლია ინფორმაციის შენახვა წარსული შემოწმებიდან და სკანირების ასაჩქარებლად ქეშის გამოყენება;
სისტემას გააჩნია ჩაშენებული მოდული ექსპლოიტების აღმოსაფხვრელად;
სისტემას შეუძლია ოპერაციული სისტემის და გავრცელებული პროგრამების სისუსტეების სიგნატურების (ხელწერის) რეგულარული განახლებები შეღწევადობის გამაფრთხილებელი ჩაშენებული მოდულით;
სისტემას შეუძლია ფაილის საკონტროლო ჯამის რეპუტაციის ღრუბლოვანი ანალიზი;
სისტემას შეუძლია სიგნატურული (ხელწერის) და ღრუბლოვანი ანალიზის შედეგებისგან დამოუკიდებლად პოტენციურად საფრთხის შემცველი აპლიკაციის ქმედების ბლოკირება;
სისტემას შეუძლია ვებ-გვერდების და საფოსტო შეტყობინებების აქტიური შევსების შემოწმება;
სისტემას შეუძლია ანტივირუსული მოდულების (ინდივიდუალური ან/და ყველა) პარამეტრების პაროლით დაცვა;
სისტემას შეუძლია რეპუტაციის ლოკალური სერვერიდან ფაილის რეპუტაციის შესახებ ინფორმაციის მიღება;

ფაერვოლი მხარდაჭერილია სწავლების და ავტომატიზებული მუშაობის რეჟიმით;
სისტემას შეუძლია გავრცელებული პროგრამებისთვის ჩაშენებული წესების არსებობა (OS, საოფისე პროგრამები და ინტერნეტ აპლიკაციები);
სისტემას გააჩნია შეღწევადობის აღმომჩენი სისტემა გაშვებული პროცესების მეხსიერების კონტროლით;
სისტემას შეუძლია იმ ოპერაციული სისტემებისა და პროგრამების დაცვა, რომლებიც გარკვეული მიზეზების გამო ხშირად ვერ იღებენ განახლებებს;
სისტემას შეუძლია URL-ის რეპუტაციაზე შემოწმება;
სისტემას შეუძლია გარკვეული კატეგორიის წყაროებზე წვდომის ბლოკირება;
სისტემას შეუძლია ე.წ. „შავი სიის" შექმნა URL-ის რეპუტაციისაგან დამოუკიდებლად;
სისტემას შეუძლია აპლიკაციის ან/და სკრიპტების გაშვების ბლოკირება დროებითი ფაილების კატალოგებიდან;
სისტემას შეუძლია ავტომატური გაშვების სიაში აპლიკაციის რეგისტრაციის მცდელობის ბლოკირება;
სისტემას შეუძლია ციფრული ხელმოწერის გარეშე გაშვებული აპლიკაციების ბლოკირება;
სისტემას შეუძლია ფაილური სისტემის და რეესტრის დონეზე დაცვის საკუთარი წესების შექმნის შესაძლებლობა;
სისტემას შეუძლია ბრაუზერების, ქსელის პარამეტრების და ფაილური ასოციაციების ცვლილებებისაგან დაცვა;
სისტემას შეუძლია გარე მატარებლების (USB) მონიტორინგი; სისტემას შეუძლია გარე მატარებლების (USB) იძულებით ბლოკირება; სისტემას შეუძლია გარე მატარებლების (USB) გადაყვანა "read-only" რეჟიმში;
სისტემას შეუძლია გარე მატარებლების (მოდემების, გაფართოების ბარათების და ა.შ.) მონიტორინგი და ბლოკირება;
სისტემას შეუძლია გარე მატარებლებზე და გარე მატარებლებიდან დოკუმენტების ჩაწერა/კოპირების მცდელობის ბლოკირება, რომელიც ემთხვევა კლიენტის მიერ მითითებულ ციფრულ ანაბეჭდებს და შეიცავენ სიტყვებს და განსაზღვრულ ფრაზებს;
სისტემას შეუძლია გამოყენებაზე თვალთვალის და ბლოკირების შესაძლებლობა;
სისტემას შეუძლია მყარი დისკებზე(სისტემური) თვალთვალის და ბლოკირების შესაძლებლობა;
სისტემას აქვს ინფორმაციის მოხსნადი მოწყობილობა არსებული ფაილებზე წვდომის (წაკითხვის) ბლოკირების შესაძლებლობა;
სისტემას შეუძლია ლოკალურ და დომენურ მომხმარებლებზე წესების გავრცელება;

ლიცენზიების რაოდენობა:	არანაკლებ 1000 ცალი. 1000 ცალი

2.4 საფრთხეების ღრუბლოვანი სერვისი

SIEM-ს გააჩნია მოდული, რომელიც IP-ის რეპუტაციას განსაზღვრავს მსოფლიოში განლაგებულ სენსორებზე დაყრდნობით, რომელიც ავტომატურად განახლებადია;
SIEM-ს გააჩნია მოდული და ფუნქციონალი, რომელიც მოახდენს საბოლოო წერტილის საეჭვო და ცუდი რეპუტაციის წყაროსთან კავშირის აღმოჩენას და დაბლოკვას წინასწარ განსაზღვრული წესების მიხედვით;
SIEM-ის მოდულს აქვს ფუნქციონალი, IP-ის რეპუტაცია ავტომატურად ჩართოს რისკის ქულის გამოთვლაში;

2.5 საფრთხეებისგან დაცვის სისტემა („სენდბოქსი“)

სისტემის ინსტალაცია ხდება ვირტუალურ გარემოში (ESXi);
სისტემით მხარდაჭერილია დინამიური ანალიზის შესაძლებლობა. კერძოდ, ფაილის გაშვება ხდება ლოკალურად ვირტუალური სენდბოქსის სისტემის გარემოში, რომ მოხდეს განსაზღვრა არის თუ არა ფაილი ზიანის მომტანი;
სისტემას დამატებით გააჩნია საფრთხეების ღრუბლოვანი სერვისთან ინტეგრაცია IP რეპუტაციების ბაზის მისაღებად;
სისტემას შეუძლია დაინფიცირებული სადგურების იდენტიფიცირება და რემედიაცია. კერძოდ, მოახდინოს იდენტიფიცირება სადგურის, საიდანაც მოხდა მავნე კოდის გაშვება და ასევე იმ სადგურების, სადაც მოხდა მავნე კოდის გავრცელება;
სისტემას შეუძლია ინტეგრაცია SIEM გადაწყვეტილებასთან, რეპუტაციის ლოკალურ სერვერთან და დაინფიცირებული სისტემების რეაგირების ქვესისტემასთან. აღნიშნულ სისტემებისთვის რეალურ დროში შესაძლებელია ინფორმაციის გაზირება საფრთხის შემცველი ფაილების შესახებ, რაც უზრუნველყოფს დაინფიცირებული სადგურების კარანტინში მოთავსებას მათ სრულ რემედიაციამდე;
მხარდაჭერილი სისტემები: Windows ვერსია 7 და ზემოთ;
მხარდაჭერილი ფაილების ტიპები: Adobe, MS Office, Archives, Java.

2.6 კომუნიკაციის საერთო მექანიზმი

SIEM გადაწყვეტილებას, სამუშაო სადგურებსა და სენდბოქსის სისტემას, აქვს ინფორმაციის ნაკადის გაზიარების მხარდაჭერა კომუნიკაციის საერთო მექანიზმით;			
კომუნიკაციის საერთო მექანიზმი მოიცავს ინფორმაციას: საფრთხის შემცველი ინდიკატორების (IOCs) შესახებ, ფაილისა და აპლიკაციების რეპუტაციების ცვლილების შესახებ, ქსელისა თუ მომხმარებლების ქმედებების შესახებ;			
აღნიშნული მექანიზმი საშუალებას იძლევა ტექნიკურ დავალებაში არსებულ სისტემებს შორის მოხდეს ინფორმაციის რეალურ დროში მიმოცვლა შემდგომში ავტომატური რეაგირების წესების ამოქმედებისთვის.			
3. ერთიანი სისტემის საინსტალაციო სამუშაოები			
მართვის ძირითადი სისტემა:	სისტემის ინსტალაცია და ქსელის პარამეტრების კონფიგურაცია;		
	განახლებების ინსტალაცია (არსებობის შემთხვევაში);		
	ლიცენზიების აქტივაცია;		
	ღრუბლოვან სერვისთან დაკავშირება;		
	Active Directory-სთან ინტეგრაცია;		
	SIEM გადაწყვეტილების სისტემის ინტეგრაცია;		
	10-მდე Data Source-ის დაკავშირება;		
	სენდბოქსიდან ხდომილებების მიღების კონფიგურირება;		
	სისტემებიდან Syslog მოვლენების მიღება;		
	MS Windows სისტემებიდან მოვლენების მიღება;		
	საჩვენებელი რეპორტების გენერაცია.		
ხდომილებების მიმღები სისტემა:	სისტემის ინსტალაცია და ქსელის პარამეტრების კონფიგურაცია;		
	მართვის ძირითად სისტემასთან დაკავშირება.		
კორელაციის სისტემა:	სისტემის ინსტალაცია და ქსელის პარამეტრების კონფიგურაცია;		
	მართვის ძირითად სისტემასთან დაკავშირება.		
ჟურნალების მართვის სისტემა:	სისტემის ინსტალაცია და ქსელის პარამეტრების კონფიგურაცია;		
	მართვის ძირითად სისტემასთან დაკავშირება.		
აპლიკაციების მონიტორინგი:	სისტემის ინსტალაცია და ქსელის პარამეტრების კონფიგურაცია;		
	მართვის ძირითად სისტემასთან დაკავშირება.		
სამუშაო სადგურების ცენტრალური მართვის კონსოლი:	სისტემის ინსტალაცია და ქსელის პარამეტრების კონფიგურაცია;		
	ლიცენზიების აქტივაცია;		

	Active Directory-სთან ინტეგრაცია (მოწოდების შემთხვევაში);
	10-მდე სამუშაო სადგურზე დაცვის სისტემების ინსტალაცია;
	სამუშაო სადგურის დაცვის სისტემების წესების ბაზური კონფიგურაცია;
	განახლებების ინსტალაცია (არსებობის შემთხვევაში);
	საჩვენებელი რეპორტების გენერაცია.
რეპუტაციის ლოკალური სერვერი:	სისტემის ინსტალაცია და ქსელის პარამეტრების კონფიგურაცია.
საფრთხეებისგან დაცვის სისტემა („სენდბოქსი“)	სისტემის ინსტალაცია და ქსელის პარამეტრების კონფიგურაცია;
საფრთხეების ღრუბლოვანი სერვისი:	სერვისის აქტივაცია და სისტემებთან დაკავშირება.
ყველა საინტალაციო სამუშაო განხორციელდება შემსყიდველის7 ოფისში, IT და OT ინფრასტრუქტურის გამოყენებით, VPN კავშირის გარეშე.	

საქონელი უნდა იყოს ექსპლუატაციაში არ მყოფი, ქარხნული , არ უნდა იყოს აღდგენილი და მეორადი.

“შემსყიდველი”:

სს ,,საქართველოს სახელმწიფო ელექტრონული სისტემა“

დავით ცირდიაშვილი
მმართველთა ხარჯოს წევრი

JSC Georgian State Electrosystem
Digitally signed by JSC Georgian State Electrosystem
Date: 2019.11.25 14:58:47 +04'00'

“მიმწოდებელი”:

შპს ,,იუჯითი”

ერმილე სულაძე
გენერალური დირექტორი

BANK OF GEORGIA
BUSINESS

ხელშეკრულების შესრულების საბანკო გარანტია # PE45557-19

თბილისი 13 ნოემბერი 2019 წელი

გარანტი: სს საქართველოს ბანკი (შემდგომში „გარანტი")
გარანტის საიდენტიფიკაციო კოდი: 204378869
გარანტის მისამართი: გაგარინის ქ. #29ა, თბილისი, 0160, საქართველო
პრინციპალი: შპს იუ-ჯი-თი (შემდგომში „პრინციპალი")
პრინციპალის საიდენტიფიკაციო კოდი: 204892964
პრინციპალის წისამართი: საქართველო, თბილისი, ვაკის რაიონი, ჭავჭავაძის გამზირი №17ა
ბენეფიციარი: სს საქართველოს სახელმწიფო ელექტროსისტემა (შემდგომში „ბენეფიციარი")
ბენეფიციარის საიდენტიფიკაციო კოდი: 204995176
საგარანტიო თანხა: 2,620 (ორი ათას ექვსასოცი) აშშ დოლარი
ტენდერის უნიკალური ნომერი: #SPA190004447

მხედველობაში ვიღებთ რა, რომ პრინციპალმა ინფორმაციული უსაფრთხოების სისტემის (თანმდევი მომსახურებით) მიწოდების მიზნით წარდგენილი სატენდერო წინადადების შესაბამისად იკისრა ვალდებულება წარმოადგინოს საბანკო გარანტია მასზე დაკისრებული ვალდებულებების შესრულების გარანტიის სახით ხელშეკრულებაში მითითებულ თანხაზე, ჩვენ, გარანტი, თანახმა ვართ გავცეთ პრინციპალის სახელზე აღნიშნული უპირობო და გამოუთხოვადი საბანკო გარანტია.

ამასთან დაკავშირებით, ვადასტურებთ, რომ ვართ გარანტები და პასუხისმგებლები თქვენს წინაშე პრინციპალის სახელით საერთო თანხაზე, არაუმეტეს ჯამში 2,620 (ორი ათას ექვსასოცი) აშშ დოლარი და ვკისრულობთ ზემოთ აღნიშნული თანხის, გადახდას პრინციპალის მიერ ხელშეკრულების პირობების დარღვევის შემთხვევაში ბენეფიციარის პირველივე წერილობითი მოთხოვნის წარმოდგენის საფუძველზე, მოთხოვნის მიღებიდან მომდევნო 5 (ხუთი) საბანკო დღის ვადაში.

ბენეფიციარის წერილობითი მოთხოვნა თანხის ანაზღაურებაზე წარმოდგენილ უნდა იქნეს ბენეფიციარის მხრიდან აღნიშნულ დოკუმენტზე უფლებამოსილი პირის მიერ ხელმოწერილი ფორმით, სადაც მითითებულ იქნება მოთხოვნილი თანხა ციფრობრივად და სიტყვიერად. საბანკო რეკვიზიტები და განმარტებული უნდა იყოს კონკრეტულად პრინციპალსა და ბენეფიციარს შორის გაფორმებული ხელშეკრულების რა პირობები იქნა დარღვეული პრინციპალის მხრიდან დამატებითი მტკიცებულების წარმოდგენის საჭიროების გარეშე. მოთხოვნას თან უნდა ერთვოდეს მოთხოვნაზე ხელმომწერი პირის უფლებამოსილების დამადასტურებელი დოკუმენტი (ბანკი უფლებამოსილია არ მოითხოვოს აღნიშნული საბუთი, თუ ხელმომწერი პირის უფლებამოსილების შესახებ ინფორმაცია საჯაროდ ხელმისაწვდომია) და საბანკო გარანტიის ასლი.

წინამდებარე გარანტია ძალაშია პრინციპალის მიერ ხელშეკრულების პირობების შესრულების საბოლოოდ დამთავრებამდე, მაგრამ არაუგვიანეს: 18 მაისი 2020 წელი, შესაბამისად წინამდებარე გარანტია მოქმედებს აღნიშნული თარიღის ჩათვლით.

ზემოთქმულიდან გამომდინარე, ბენეფიციარის მიერ წარმოდგენილი წერილობით მოთხოვნის ორიგინალი დოკუმენტი თანხის ანაზღაურებაზე, გარანტის მიერ მიღებულ უნდა იქნას გარანტიის მოქმედების ვადის ჩათვლით სს "საქართველოს ბანკის" სათავო ოფისში, კანცელარიის სამსახურში, ვაჭრობის სტრუქტურული დაფინანსების დეპარტამენტის საყურადღებოდ, თბილისის დროით (UTC / GT +04: 00 საათი) 17:00 საათის ჩათვლით, შემდეგ მისამართზე: გაგარინის ქ.#29ა, თბილისი 0160, საქართველო.

საბანკო გარანტია ავტომატურად უქმდება/მცირდება ქვემოაღნიშნული გარემოებებიდან ერთ-ერთის დადგომისთანავე:

- საბანკო გარანტიის ვადის გასვლით;
- გარანტის მიერ ბენეფიციარისთვის იმ თანხის გადახდით, რომელზედაც გაიცა საბანკო გარანტია;
- ბენეფიციარის მიერ გარანტიიდან გამომდინარე თავის უფლებებზე წერილობით უარის თქმით;
- ბენეფიციარის მიერ საბანკო გარანტიის თანხის შემცირების შესახებ წერილობითი შეტყობინებით.

გარანტის მიმართ საბანკო გარანტიიდან გამომდინარე ბენეფიციარის კუთვნილი მოთხოვნის უფლების გადაცემა/დათმობა სხვა პირისათვის დაუშვებელია გარანტის წერილობითი თანხმობის გარეშე.

წინამდებარე საბანკო გარანტია რეგულირდება საქართველოს კანონმდებლობით.

პატივისცემით,
ვთერ ხეიშვილი
ადგილობრივი გარანტიების სამსახურის უფროსი

სს „საქართველოს ბანკი"
გაგარინის ქ. №29ა
თბილისი 0160, საქართველო

JSC Bank of Georgia
29A Gagarini Str.,
Tbilisi 0160, Georgia

documents@bog.ge | trade_finance@bog.ge | (0 32) 2 444 444

BANK OF GEORGIA
BUSINESS

#PE45557-19 საბანკო გარანტიაში ცვლილების თაობაზე 001- შეტყობინება

თბილისი 21 ნოემბერი 2019 წელი

გარანტი: სს „საქართველოს ბანკი“ (შემდგომში „გარანტი“)
გარანტის საიდენტიფიკაციო კოდი: 204378869
გარანტის მისამართი: გაგარინის ქ. #29ა, თბილისი, 0160, საქართველო
პრინციპალი: შპს იუ-ჯი-თი (შემდგომში „პრინციპალი“)
პრინციპალის საიდენტიფიკაციო კოდი: 204892964
პრინციპალის მისამართი: საქართველო, თბილისი, ვაკის რაიონი, ჭავჭავაძის გამზირი №17ა
ბენეფიციარი: სს საქართველოს სახელმწიფო ელექტროსისტემა (შემდგომში „ბენეფიციარი“)
ბენეფიციარის საიდენტიფიკაციო კოდი: 204995176
გარანტიის ახალი თანხა: 3,100 (სამი ათას ასი) აშშ დოლარი

ბატონებო,

გაცნობებთ, რომ 2019 წლის 13 ნოემბერს პრინციპალის დავალებით ჩვენს მიერ გაცემულ #PE45557-19 საბანკო გარანტიაში შევიდა შემდეგი ცვლილება:

1. საბანკო გარანტიის თანხა გაიზარდა და დღეის მდგომარეობით შეადგენს 3,100 (სამი ათას ასი) აშშ დოლარს.

#PE45557-19 საბანკო გარანტიის ყველა დანარჩენი პირობა დარჩა უცვლელი.

პატივისცემით,
გიორგი ხეიშვილი
ადგილობრივი გარანტიების დეპარტამენტის უფროსი

BANK OF GEORGIA
204378869
STRUCTURED FINANCE DEPARTMENT

სს „საქართველოს ბანკი“
გაგარინის ქ. №29
თბილისი 0160, საქართველო

JSC Bank of Georgia
29A Gagarini Str.,
Tbilisi 0160, Georgia

documents@bog.ge | trade_finance@bog.ge | (032) 2 444 444