ხელშეკრულება № 01-41
სახელმწიფო შესყიდვების შესახებ
CPV – 32400000 - ქსელები
CPV- 32424000 - ქსელის ინფრასტრუქტურა

ქ. თბილისი 13 აგვისტო 2018 წელი

ერთი მხრივ სსიპ განათლების მართვის საინფორმაციო სისტემა (შემდგომში „შემსყიდველი"), წარმოდგენილი უფროსის **დიმიტრი ბერიძის** სახით და მეორე მხრივ **შპს „იუ ჯი თი"** (შემდგომში „მიმწოდებელი") წარმოდგენილი გენერალური დირექტორის **ერმილე სულაბის** სახით, შემსყიდველის მიერ უსაფრთხოების სისტემის თანმდევი ინსტალაციით შესყიდვის მიზნით 2018 წლის 16 ივლისს გამოცხადებული **SPA180006286** ელექტრონული ტენდერისა და სახელმწიფო შესყიდვების შესახებ კანონის საფუძველზე, დებენ წინამდებარე ხელშეკრულებას შემდეგზე:

1. ტერმინთა განმარტება

1.1. „ხელშეკრულება სახელმწიფო შესყიდვის შესახებ" - შემსყიდველსა და ტენდერში გამარჯვებულ პრეტენდენტს შორის დადებული ხელშეკრულება, რომელიც ხელმოწერილია მხარეთა მიერ, მასზე თანდართული ყველა დოკუმენტით და დამატებებით, ასევე, სატენდერო დოკუმენტაციის პირობებით და იმ დოკუმენტაციით, რომლებზეც ხელშეკრულებაში არის მინიშნებები.

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

1.3. „დღე", „კვირა", „თვე" – კალენდარული დღე, კვირა, თვე.

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

1.5. „მიმწოდებელი" – პირი, რომელიც ახორციელებს საქონლის მიწოდებას ხელშეკრულების ფარგლებში.

1.6. „შესყიდვის ობიექტი" – ხელშეკრულების მე-2 მუხლით გათვალისწინებული ხელშეკრულების საგანი.

1.7. „ტექნიკური დავალება" – **N SPA180006286** ელექტრონული ტენდერის სატენდერო დოკუმენტაციის ტექნიკური დავალება, რომელიც დაერთვება ხელშეკრულებას, როგორც მისი განუყოფელი ნაწილი.

2. ხელშეკრულების საგანი

2.1. ხელშეკრულების საგანია უსაფრთხოების სისტემის (საქონელი) შესყიდვა თანმდევი ინსტალაციით, წინამდებარე ხელშეკრულებით გათვალისწინებული პირობების შესაბამისად.

2.2 . საქონლის დასახელება, მწარმოებელი კომპანია, მწარმოებელი ქვეყანა, მოდელი, რაოდენობა ერთეულის და საერთო ფასი განისაზღვრება წინამდებარე ხელშეკრულების დანართი N1-ის შესაბამისად.

2.3. შესყიდვის ობიექტის აღწერა და პირობები (ტექნიკური დავალება) განისაზღვრება წინამდებარე ხელშეკრულების დანართ N2-ში.

3. ხელშეკრულების ღირებულება და ანგარიშსწორების პირობები

3.1.ხელშეკრულების ჯამური (საერთო) ღირებულება შეადგენს: 994 500,00 (ცხრაასოთხმოცდათოთხმეტი ათას ხუთასი ლარი და 00 თეთრი) ლარს (დღგ-ს ჩათვლით).

3.2. ხელშეკრულების ღირებულება მოიცავს შესყიდვის ობიექტის მიწოდებასთან დაკავშირებულ მიმწოდებლის ყველა ხარჯს და საქართველოს კანონმდებლობით გათვალისწინებულ გადასახადებს.

3.3. ანგარიშსწორება მოხდება უნაღდო ანგარიშსწორებით, ლარში.

3.4. ანგარიშსწორება განხორციელდება წარმოდგენილი ანგარიშ-ფაქტრის საფუძველზე, მიღება-ჩაბარების აქტის გაფორმებიდან 10 (ათი) სამუშაო დღეში.

3.5. დაფინანსების წყარო: **2018 წლის საბიუჯეტო სახსრები.**

3.6. მიმწოდებლის მოთხოვნისა და შემსყიდველის თანხმობით, შესაძლებელია განხროციელდეს წინასწარი საავანსო გადახდა, ხელშეკრულების ჯამური (საერთო) ღირებულების 80%-ისა, იდენტური შესაბამისი საბანკო გარანტიის საფუძველზე, საბანკო გარანტიის წარმოდგენიდან 10 (ათი) სამუშაო დღეში. (საბანკო გარანტიის ვადა უნდა აღემატებოდეს შესყიდვის ობიექტის მიწოდების ვადას არანაკლებ 30 (ოცდაათი) კალენდარული დღით).

4. ხელშეკრულების მოქმედების ვადები

ხელშეკრულება ძალაში შედის მხარეთა უფლებამოსილი წარმომადგენლების ხელმოწერის დღიდან და მოქმედებს 2019 წლის 31 იანვარის ჩათვლით.

5. შესყიდვის ობიექტის მიწოდების პირობები

საქონლის მიწოდება თანმდევი ინსტალაციით უნდა განხორციელდეს ხელშეკრულების გაფორმებიდან 80 (ოთხმოცი) კალენდარული დღის განმავლობაში, შემდეგ მისამართზე: ქ. თბილისი, ფანჯიკიძის ქ. N1ა.

6. ხელშეკრულების ინსპექტირება

6.1. შემსყიდველი ახორციელებს კონტროლსა და ზედამხედველობას მიმწოდებლის მიერ ხელშეკრულების პირობების შესრულებაზე.

6.2. ამ მუხლის პირველი პუნქტით გათვალისწინებული კონტროლისა და ზედამხედველობის განმახორციელებელ პირს, შემსყიდველის მხრიდან, წარმოადგენს სსიპ განათლების მართვის საინფორმაციო სისტემის კომპიუტერული სისტემების, ქსელებისა და კომუნიკაციის სამსახურის ქსელური და სისტემური ინფრასტრუქტურის არქიტექტორი **როსტომ ნებიერიძე** ან სსიპ განათლების მართვის საინფორმაციო სისტემის კომპიუტერული სისტემების, ქსელებისა და კომუნიკაციის სამსახურის ქსელის ადმინისტრატორი **ბესარიონ ბარაბაძე**.

7. შესყიდვის ობიექტის მიღება-ჩაბარების წესი

7.1 ხელშეკრულებით გათვალისწინებული საქონლის თანმდევი ინსტალაციით მიღება დასტურდება მხარეებს შორის მიღება-ჩაბარების აქტის გაფორმებით, მას შემდეგ რაც მიმწოდებლის მიერ წარმოდგენილი იქნება შესაბამისი სასაქონლო ზედნადები და შემსყიდველის მხრიდან ინსპექტირებისას არ იქნება გამოვლენილი საქონლის და თანმდევი ინსტალაციის რაიმე ნაკლი ან ხარვეზი.

7.2. შემსყიდველი ვალდებულია ინსპეტირება განახორციელოს საქონლის (თანმდევი ინსტალაციით) გადაცემიდან არაუგვიანეს 7 (შვიდი) სამუშაო დღისა. საქონლის გადაცემიდან ინსპექტირების დასრულებამდე/მიღება-ჩაბარების აქტის გაფორმებამდე, საქონლის შენახვის პასუხისმგებლობა ეკისრება შემსყიდველს.

7.3 შემსყიდველის მხრიდან მიღება-ჩაბარების აქტის ხელმოწერაზე პასუხისმგებელი პირია სსიპ განათლების მართვის საინფორმაციო სისტემის ფინანსური და მატერიალური რესურსების სამსახურის უფროსის მოადგილე **ნიკოლოზ ლომსაძე** ან სსიპ განათლების მართვის საინფორმაციო სისტემის უფროსის 2018 წლის 3 აპრილის N1.1/151 ბრძანებით განსაზღვრული პირი.

8. მხარეთა ვალდებულებები და პასუხისმგებლობა

8.1 მიმწოდებელი ვალდებულია უზრუნველყოს ხელშეკრულებით განსაზღვრული საქონლის (თანმდევი ინსტალაციით) მიწოდება უნაკლოდ. თუკი შესყიდვის ობიექტი არ აღმოჩნდება სრულყოფილი, მიმწოდებელი ვალდებულია, შემსყიდველის მოთხოვნისთანავე (გონივრულ ვადაში), გამოასწოროს ეს ნაკლი.

8.2 მიმწოდებელი უფლებამოსილია მოსთხოვოს შემსყიდველს შესყიდვის ობიექტის ღირებულების ანაზღაურება ხელშეკრულებით გათვალისწინებული ვადებისა და პირობების დაცვით.

8.3 შემსყიდველი ვალდებულია გადაიხადოს შესყიდვის ობიექტის ღირებულება ამ ხელშეკრულებით გათვალისწინებული პირობებით.

8.4 შემსყიდველი უფლებამოსილია ნებისმიერ დროს განახორციელოს მიმწოდებლის მიერ ნაკისრი ვალდებულებების შესრულებისა და ხარისხის ინსპექტირება.

8.5 ფორსმაჟორული გარემოებების გარდა ხელშეკრულებით გათვალისწინებული ვალდებულებების შესრულების ვადების გადაცდენის შემთხვევაში მხარეებს დაეკისრება პირგასამტეხლოს გადახდა ყოველ ვადაგადაცილებულ დღეზე - ხელშეკრულების საერთო ღირებულების 0,02%-ის ოდენობით.

8.6 პირგასამტეხლოს გადახდა არ ათავისუფლებს მხარეებს ძირითადი ვალდებულებების შესრულებისაგან.

8.7 იმ შემთხვევაში, თუ მხარისათვის დაკისრებული პირგასამტეხლოს ჯამური თანხა გადააჭარბებს ხელშეკრულების საერთო ღირებულების 1 (ერთი) პროცენტს, მეორე მხარეს უფლება აქვს ცალმხრივად მოითხოვოს ხელშეკრულების შეწყვეტა და მიყენებული ზიანის ანაზღაურება, ასევე, შეუსრულებელი ვალდებულების გამო, მხარეს დაეკისრება პირგასამტეხლო ხელშეკრულების საერთო ღირებულების 10%-ის ოდენობით.

9. საგარანტიო პირობები

9.1. მიწოდებულ საქონელზე ვრცელდება საგარანტიო მომსახურება მხარეებს შორის შესყიდვის ობიექტის მიღება-ჩაბარების აქტის გაფორმებიდან 2 (ორი) წლის განმავლობაში.

9.2. საგარანტიო ვადაში მიმწოდებელი ვალდებულია უფასოდ განახორციელოს საქონლის შეკეთება, იმ შემთხვევაში თუ მიწოდებული საქონელი არ ექვემდებარება შეკეთებას, უნდა განხორციელდეს მისი შეცვლა.

9.3. გადაწყვეტილების კომპონენტებზე ვრცელდება მინიმუმ 2 (ორი) წლიანი მწარმოებლის გარანტია.

9.4. გადაწყვეტილებაზე ვრცელდება მინიმუმ 2 (ორი) წლიანი მწარმოებლის მხარდაჭერა, რომელიც განხორციელდება პირდაპირ მწარმოებელთან კომუნიკაციით.
9.5. მწარმოებლმა უნდა უზრუნველყოს ტექნიკური მხარდაჭერა 7 x 24-ზე (ყოველ დღე).
9.6. გადაწყვეტილებაზე ვრცელდება პროგრამული უზრუნველყოფის და სხვა აუცილებელი კომპონენტების მინიმუმ 2 (ორი) წლიანი განახლებების სერვისი.
9.7. მიმწოდებელი თავისუფლდება ზემოხსენებული მოვალეობის შესრულებისაგან, თუ დადგინდა, რომ დაზიანება შემსყიდველის პერსონალის ბრალითაა გამოწვეული.

10. ხელშეკრულების შესრულების გარანტია
10.1 იმისათვის, რომ თავიდან იქნას აცილებული მიმწოდებლის მიერ სახელმწიფო შესყიდვის შესახებ ხელშეკრულების პირობების შეუსრულებლობის რისკი, გამოიყენება ხელშეკრულების შესრულების უზრუნველყოფის საბანკო გარანტია.
10.2. ვინაიდან, მიმწოდებელი წარმოადგენს „თეთრ სიაში“ მყოფ იურიდიულ პირს, ხელშეკრულების შესრულების უზრუნველყოფის საბანკო გარანტია წარმოდგენილია წინამდებარე ხელშეკრულების საერთო ღირებულების 1,5 %-ით. საბანკო გარანტია გაცემულია 2018 წლის 7 აგვისტოს სს „საქართველოს ბანკის“ მიერ (PE42993-18) 14 917.50 (თოთხმეტი ათას ცხრაასჩვიდმეტი ლარი და 50 თეთრი) ლარის ოდენობით, 2019 წლის 30 იანვრის ჩათვლით მოქმედების ვადით.
10.2 მიმწოდებელს, მისი წერილობითი მოთხოვნის საფუძველზე, ხელშეკრულების შესრულების უზრუნველსაყოფად გაცემული საბანკო გარანტია, ხელშეკრულებით გათვალისწინებული ვალდებულებების უნაკლოდ შესრულების შემთხვევაში, დაუბრუნდება მხარეთა შორის შესყიდვის ობიექტის მიღება-ჩაბარების აქტის გაფორმების შემდეგ.
10.3 მიმწოდებლისაგან დამოუკიდებელი მიზეზების გამო ხელშეკრულების შეწყვეტის შემთხვევაში, შემსყიდველი ვალდებულია მიმწოდებლის მოთხოვნისთანავე, დაუბრუნოს მას ხელშეკრულების შესრულების უზრუნველყოფის გარანტია.

11. ფორს-მაჟორი
11.1. მხარეებს არ დაეკისრებათ პასუხისმგებლობა ხელშეკრულებით გათვალისწინებული ვალდებულებების შეუსრულებლობის ან ვადის გადაცილებისათვის თუკი, შეუსრულებლობა გამოწვეულია ფორს-მაჟორული გარემოებებით.
11.2. ამ მუხლის მიზნებისათვის ფორს-მაჟორი ნიშნავს ისეთ გარემოებებს, რომელთა არსებობის გამო მხარისათვის ობიექტურად შეუძლებელი იყო სახელშეკრულებო ვალდებულებების შესრულება (სტიქიური მოვლენები, საომარი მოქმედება, ეპიდემია, კარანტინი, საბიუჯეტო ასიგნებების მკვეთრი შემცირება, საქონლის მიწოდებაზე ემბარგოს დაწესება, სახელწიფო გადატრიალება და სხვ.).
11.3. ფორს-მაჟორული გარემოებების დადგომის შემთხვევაში ხელშეკრულების მხარემ, რომლისთვისაც შეუძლებელი ხდება ნაკისრი ვალდებულებების შესრულება, პირველი შესაძლებლობისთანავე უნდა გაუგზავნოს მეორე მხარეს წერილობითი შეტყობინება ასეთი გარემოებების და მათი გამომწვევი მიზეზების შესახებ. თუ შეტყობინების გამგზავნი მხარე არ მიიღებს მეორე მხარისაგან პასუხს, იგი თავისი შეხედულებისამებრ, მიზანშეწონილობისა და შესაძლებლობის მიხედვით აგრძელებს ხელშეკრულებით ნაკისრი ვალდებულებების შესრულებას და ცდილობს გამონახოს ვალდებულების შესრულების ისეთი ალტერნატიული ხერხები, რომლებიც დამოუკიდებელი იქნებიან ფორს-მაჟორული გარემოებებისაგან.

12. ხელშეკრულებაში ცვლილებების შეტანის და შეწყვეტის წესი
12.1. ხელშეკრულებაში ნებისმიერი ცვლილების, დამატების შეტანა შესაძლებელია მხოლოდ მხარეთა შორის წერილობითი ფორმით შედგენილი შეთანხმების საფუძველზე.
12.2. ხელშეკრულების პირობების, მათ შორის, ფასის შეცვლა დაუშვებელია, თუ ამ ცვლილებების შედეგად იზრდება ხელშეკრულების ჯამური ღირებულება ან უარესდება ხელშეკრულების პირობები შემსყიდველისთვის, გარდა საქართველოს სამოქალაქო კოდექსის **398**-ე მუხლით გათვალისწინებული შემთხვევებისა. ხელშეკრულების პირობების გადასინჯვა ხდება საქართველოს კანონმდებლობით დადგენილი წესით.
12.3. საქართველოს სამოქალაქო კოდექსის 398–ე მუხლით გათვალისწინებული გარემოებების დადგომის შემთხვევაში, ხელშეკრულების ჯამური ღირებულების გაზრდა დაუშვებელია ხელშეკრულების ღირებულების **10%-ზე** მეტი ოდენობით.
12.4. ხელშეკრულების ერთ-ერთი მხარის მიერ ხელშეკრულების პირობების შეუსრულებლობის შემთხვევაში მეორე მხარე უფლებამოსილია ცალმხრივად მიიღოს გადაწყვეტილება ხელშეკრულების შეწყვეტის შესახებ.
12.5. ხელშეკრულების 12.4 პუნქტით გათვალისწინებულ შემთხვევაში ინიციატორი მხარე ვალდებულია გადაწყვეტილების მიღების განზრახვის შესახებ არანაკლებ 10 (ათი) სამუშაო დღით ადრე წერილობით აცნობოს ამის შესახებ მეორე მხარეს.

13. დავების გადაჭრის წესი

ამ ხელშეკრულების შესრულების დროს წამოჭრილი ყველა დავა შეძლებისდაგვარად გადაიჭრება მხარეთა შორის მოლაპარაკების გზით. შეთანხმების მიუღწევლობის შემთხვევაში დავას წყვეტს სასამართლო.

14. დასკვნითი დებულებები

ხელშეკრულება შედგენილია თანაბარი იურიდიული ძალის მქონე სამ ეგზემპლარად ქართულ ენაზე (ორი რჩება შემსყიდველს, ერთი – მიმწოდებელს).

15. მხარეთა რეკვიზიტები:

შემსყიდველი:	**მიმწოდებელი:**
სსიპ განათლების მართვის	შპს „იუ ჯი თი”
საინფორმაციო სისტემა	
ს.კ. 205300048	ს.კ. 204892964
მისამართი: ქ. თბილისი, ფანჯიკიძის ქუჩა N1ა	მისამართი: თბილისი, ჭავჭავაძის გამზ. 17ა
	საბანკო რეკვიზიტები:
	სს საქართველოს ბანკი
	კოდი: BAGAGE22
	ა/ა: GE88BG0000000261644601
უფროსი	გენერალური დირექტორი
დიმიტრი ბერიძე _____ ბ.ა.	**ერმილე სულაძე** _____ ბ.ა.

დანართი N1

№	დასახელება	მწარმოებელი ქვეყანა	მწარმოებელი კომპანია (ბრენდი)	მოდელი	განზომილების ერთეული	რაოდენობა	ერთეულის ღირებულება	ჯამური ღირებულება
1	უსაფრთხოების სისტემა (თანმდევი ინსტალაციით)	ტაივანი	Check Point Software Technologies	44000 Security System	ცალი	1	994500,00	994500,00 ლარი

სსიპ განათლების მართვის საინფორმაციო სისტემა

უფროსი

დიმიტრი ბერიძე _____ ბ.ა.

შპს იუ ჯი თი

გენერალური დირექტორი

ერმილე სულაძე _____ ბ.ა.

დანართი N2

ტექნიკური დავალება

ზოგადი ტექნიკური მოთხოვნები

- შემოთავაზებული ბრენდმაუერი უნდა წარმოადგენდეს პროგრამულ-აპარატურულ გადაწყვეტილებას
- ბრენდმაუერის კონფიგურაცია უნდა შედგებოდეს ერთი შასისგან, რომელშიც შესაძლებელია განთავსდეს არანაკლებ ორი კომუტატორის მოდული, არანაკლებ 5 ბრენდმაუერის მოდული და არანაკლებ 2 მართვის მოდული.
- ბრენდმაუერის, კომუტატორის და მართვის მოდულების მწყობრიდან გამოსვლის შემთხვევაში შესაძლებელი უნდა იყოს ავტომატურად გადაირთოს მეორე დუბლირებულ მოდულებზე, წყვეტის გარეშე (High Availability).
- ბრენდმაუერის შემოთავაზებულ გადაწყვეტილებაში აუცილებელია იყოს დუბლირებული ბრენდმაუერის და კომუტატორის მოდულები.
- შემოთავაზებული გადაწყვეტილება ლიცენზირებული უნდა იყოს ულიმიტო მომხმარებლის რაოდენობაზე.
- ბრანდმაუერის მართვა შესაძლებელი უნდა იყოს შემდეგი მეთოდებით:
    - ვირტუალურ გარემოში გაშვებული მართვის მოდულით
    - მწარმოებლისგან სამართავი ფიზიკური მოწყობილობის ინტეგრაციით.
- შემოთავაზება უნდა მოიცავდეს ვირტუალური მენეჯმენტის სისტემას, საიდანაც შესაძლებელი იქნება ბრანდმაუერის შასის ცენტრალური მართვა, ლოგირება, მოვლენების ერთიანი კორელაცია და რეპორტინგი.

მოთხოვნები ბრანდმაუერის სისტემაზე

ბრანდმაუერის ტიპი	ახალი თაობის ბრანდმაუერის სისტემა - Next-Generation Firewall System
მოთხოვნები წარმადობაზე	▪ არანაკლებ 120 Gbps Firewall (1518 byte UDP) გამტარუნარიანობა - გაფართოებადი არანაკლებ 370 Gbps-მდე. ▪ არანაკლებ 42 Gbps IPS გამტარუნარიანობა - გაფართოებადი არანაკლებ 125 Gbps-მდე. ▪ არანაკლებ 20 Gbps NGFW გამტარუნარიანობა - გაფართოებადი არანაკლებ 60 Gbps-მდე (შემდეგი ფუქნციონალით: Firewall, IPS და Application Control).

	▪ არანაკლებ 1,2 მილიონი ახალი შეერთების შექმნის შესაძლებლობა წამში (Connections per second) - გაფართოებადი არანაკლებ 4,2 მილიონამდე ▪ არანაკლებ 30 მილიონი ერთდროული სესიების რაოდენობა (Concurrent Sessions) - გაფართოებადი არანაკლებ 110 მილიონამდე.
ოპტიკური გამსხივებლები	▪ არანაკლებ 8 x SFP+ transceiver for 10G fiber ports - short range (10GBase-SR) ▪ არანაკლებ 4 x Twisted-pair cabling transceiver for 1G SFP fiber ports (1000Base-T RJ45)
ქსელის პორტები	▪ არანაკლებ 8 x 10GbE ▪ არანაკლებ 4 x 40GbE ▪ არანაკლებ 2 x 100GbE
ფორმ ფაქტორი	არაუმეტეს 8RU
კვების წყარო	არანაკლებ 3 ცალი
ფუნქციონალი, რომელიც უნდა იყოს გააქტიურებული შემოთავაზებაში. დეტალური აღწერა იხ. „დეტალური ტექნიკური მოთხოვნები ფუნქციონალის მიმართ".	✓ ბრენდმაუერი - Firewall ✓ მომხმარებელთა იდენტიფიკაცია - User Identity ✓ მოშორებული VPN წვდომა - VPN (IPsec) ✓ შეღწევის პრევენციის სისტემა - IPS ✓ აპლიკაციების კონტროლი - Application Control ✓ ვებ ფილტრი - URL Filtering ✓ მავნე პროგრამებისგან დაცვა - Anti-Virus ✓ ანტი-ბოტი - Anti-Bot

მართვის სისტემა

სისტემის ტიპი	უსაფრთხოების ცენტრალური მენეჯმენტი - Security Management System
მხარდაჭერილი პლათფორმა	VMware
მოთხოვნები მართვისა და ლოგირების მიმართ	არანაკლებ 5 ბრანდმაუერის ერთდროული მართვა და ლოგების ცენტრალური ანალიზი
ფუნქციონალი, რომელიც უნდა იყოს გააქტიურებული. ფუქნციონალის დეტალური აღწერა	✓ ცენტრალური მართვა - Policy Management ✓ ლოგირება - Logging ✓ რეპორტინგი - Reporting ✓ მოვლენების კორელაცია - Event Correlation ✓ მომხმარებელთა იდენტიფიკაცია - User Identity ✓ რისკებთან და სტანდარტებთან შესაბამისობა - Governance Compliance

იხ. „დეტალური ტექნიკური მოთხოვნები ფუნქციონალის მიმართ“.	

დეტალური ტექნიკური მოთხოვნები ფუნქციონალის მიმართ

ბრენდმაუერის ფუნქციონალი - Firewall

- ბრენდმაურეი უნდა იყენებდეს Statefull ინსპექციას.
- გადაწყვეტილებას უნდა ქონდეს არანაკლებ 500 წინასწარ განსაზღვრული სერვისების და პროტოკოლების მხარდაჭერა.
- უნდა შეეძლოს გადასცეს სტატისტიკა მართვის აპლიკაციას. სტატისტიკური მონაცემები უნდა მოიცავდეს ინფორმაციას იმის შესახებ თუ რამდენჯერ მოხდა უსაფრთხოების წესის (Rule) გამოყენება (hit count statistics).
- უნდა შეეძლოს ავტომატურად უსაფრთხოების წესის (Rule) აქტივაცია/დეაქტივაცია დროის განსაზღვრულ შუალედებში.
- მართვის სერვერს და ბრენდმაუერებს შორის კომუნიკაცია უნდა იყოს დაშიფრული და აუტენთიფიკაცია უნდა ხდებოდეს PKI სერტიფიკატების გამოყენებით.
- ბრანდმაურს უნდა შეეძლოს აუტენთიფიკაცია მომხმარებლის, კლიენტის და სესიის მიხედვით.
- ბრედნმაუერის და VPN ფუნქციონალს უნდა გააჩნდეს მომხმარებლის აუტენთიფიკაციის შემდები მეთოდები: TACACS, RADIUS და ციფრული სერთიფიკატები (Digital Certificates).
- ბრენდმაუერს უნდა ჰქონდეს შესაძლებლობა მაღალმდგრადობის უზრუნველყოფის, ასევე დატვირთვების გადანაწილების და მდგომარეობის სინქრონიზაციის (State Synchronization).

მომხმარებელთა იდენტიფიკაცია - User Identity

- შესაძლებელი უნდა იყოს Microsoft Active Directory-დან მომხმარებლების იდენტიფიცირება.
- შესაძლებელი უნდა იყოს მომხმარებლის აუტენთიფიკაცია ბროუზერის გამოყენებით.
- უნდა ჰქონდეს ტერმინალ სერვერებთან ინტეგრაციის შესაძლებლობა.
- უნდა შეეძლოს მომხმარებლის საიდენტიფიკაციო მონაცემების მიღება Microsoft AD - დან სპეციალური აგენტების ინსტალაციის გარეშე.
- შესაძლებელი უნდა იყოს მომხმარებლის საიდენტიფიკაციო მონაცემების გაზიარება ან გავრცელება რამოდენიმე უსაფრთხოების ბრენდმაუერისთვის.
- შესაძლებელი უნდა იყოს იდენტიფიცირების როლების შექმნა და შემდგომ მათი გამოყენება უსაფრთხოების აპლიკაციებში.

ვირტუალური ლოკალური ქსელი - VPN (IPsec)

- მხარდაჭერა უნდა ქონდეს როგორც ლოკალური CA-ს (Certificate Authorities) და ასევე გარე მესამე მხარის CA-ს.
- გადაწყვეტილებას უნდა ქონდეს მხარდაჭერა 3DES და AES-256 cryptographic შემდეგი ფაზებისთვის IKE Phase I და II IKEv2.
- გადაწყვეტილებას უნდა ქონდეს არანაკლებ შემდეგი Diffie-Hellman-ის ჯგუფების მხარდაჭერა: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20.

- შესაძლებელი უნდა იყოს VPN-ის კონფიგურაცია GUI-თი ეგრედ წოდებული „drag and drop"-ის საშუალებით.
- ფუნქციონალს უნდა ქონდეს მხარდაჭერა L2TP VPNs.
- შესაძლებელი უნდა იყოს VPN შიდა ტრაფიკისთვის უსაფრთხოების წესების(Rule) დაწერა.
- უნდა ქონდეს მხარდაჭერა route based VPNs, VTI's და dynamic routing protocols გამოყენებით.
- შესაძლებელი უნდა იყო VPN-ის აწყობა დინამიური გლობალური IP-ის გამოყენებით.
- ფუნქციონალს უნდა შეეძლოს IP კომპრესია client-to-site და site-to-site VPNs-თვის.

აპლიკაციების კონტროლი, URL ფილტრაცია - Application Control, URL Filtering

- Application control-ის მონაცემთა ბაზა უნდა მოიცავდეს არანაკლებ 2300 ცნობად აპლიკაციას.
- უნდა იყოს შესაძლებელი რამოდენიმე კატეგორიის ერთ ფილტრაციის წესში(Rule) გაერთიანების.
- უნდა იყოს შესაძლებელი ფილტრაციის წესის შექმნა ერთი საიტისთვის რომელიც რამოდენიმე კატეგორიაშია.
- უნდა იყოს შესაძლებლობა აპლიკაციების და URL-ების რისკის ფაქტორებით კატეგორიზაცია.
- უნდა იყოს შესაძლებელი Application control-ის და URL ფილტრაციის პოლიტიკებში განიზასღვროს მომხმარებლის საიდენტიფიკაციო პარამეტრები.
- უნდა იყოს შესაძლებლობა ერთ უსაფრთხოების წესში გაიწეროს Application control-ის და URL ფილტრაციის პოლიტიკები.
- უნდა იყოს შესაძლებელი შეიზღუდოს კონკრეტული აპლიკაციის მოხმარება სიჩქარის მითითებით
- შესაძლებელი უნდა იყოს ცვლილების შეტანა შეტყობინების/გაფრთხილების გვერდში და მომხარებლის გადამისამართება წინასწარ განსაზღვულ ვებ გვერდზე.
- ფუნქციონალი უნდა მოიცავდეს თეთრ და შავი სიის მექანიზმს. სადაც შესაძლებელი იქნება ნებისმიერი URL-ის განთავსება მიუხედავად იმისა რომელ კატეგორიას განეკუთვნება ეს URL-ი.
- გადაწყვეტილებას უნდა ქონდეს კონფიგურირებადი შემოვლითი (bypass) მექანიზმი.
- Application control-ის და URL ფილტრაციის უსაფრთხოების პოლიტიკებს უნდა შეეძლოს აღრიცხვა , თუ რამდენჯერ იყო გამოყენებული თითოეული წესი (Policy Rule).
- უსაფრთხოების პოლიტიკის წესის, რომელიმე სექციაში უნდა შეიძლებოდეს კონკრეტულად ამ უსაფრთხოების წესისთვის უშუალოდ URL Category-ის მითითება ან ცვლილება, იმისათვის რომ ხდებოდეს ე.წ. "Policy match" მითითებული URL კატეგორიების მიხედვით.

შეღწევადობის პრევენცია - Intrusion Prevention System

- IPS-ი და ბრენდმაუერის ფუნქციონალი უნდა იყოს ინტეგრირებული ერთ პლატფორმაში.
- შესაძლებელი უნდა იყოს IPS შემოწმების (inspection) კონფიგურაცია ისე, რომ მხოლოდ შიდა რესურსი (Host) იქნას დაცული.
- IPS-ს უნდა მოყვებოდეს წინასწარ გამზადებული არანაკლებ 2 პროფილი/პოლიტიკა, რომელიც შეიძლება იქნას გამოყენებული მყისიერად.
- IPS-ის ახალი სიგნატურების (signatures) და განახლებების აქტივაცია და მართვა უნდა ხდებოდეს ავტომატურად.
- IPS-ს უნდა შეეძლოს ქსელის გამონაკლისების დაშვება source, destination, service ან ამ სამივე კომპონენტის კომბინირების საშუალებით.

- IPS-ს უნდა შეეძლოს შემდეგი ტიპის საფრთხეების აღმოჩენა და აღმოფხვრა წინასწარ განსაზღვრული სიგნატურების გარეშე. (Protocol misuse, malware communications, tunneling attempts და generic attack types).
- IPS-ს უნდა ქონდეს შესაძლებლობა რომ აღმოაჩინოს და დაბლოკოს Application 7-ე დონის შემოტევები, დაცული უნდა იყოს მინიმუმ ეს სერვისები: email services, DNS, FTP, Windows services, SNMP.
- IPS უნდა ჰქონდეს მექანიზმი, რომლის საშუალებიტაც სისტემაში დააკონვერტირებს SNORT-ის სინგატურებს
- შესაძლებელი უნდა იყოს IPS ინსპექტირებიდან გამონაკლისების დაშვება ქსელისთვის და ჰოსტისთვის.
- შესაძლებელი უნდა იყოს DNS Cache Poisoning -გან დაცვა და აღკვეთოს მომხმარებლების დაშვება დაბლოკილ დომეინების მისამართებზე.
- შესაძლებელი უნდა იყოს გამავალი და შემომავალი ტრაფიკის ბლოკირება ქვეყნების მიხედვით, აღნიშნული ფუნქციონალისთვის არ უნდა იყოს საჭიროება ქვეყნების IP დიაპაზონების ხელით გაწერა.

ანტი-ვირუსი, ანტი-ბოტი - Anti-Virus, Anti-bot

- Anti-Virus და Anti-bot დაფუნქციონალი სრულად უნდა იყოს ინტეგრირებული ბრენდმაუერში, სხვა დანარჩენ ფუნქციონალთან ერთად .
- Anti-Virus და Anti-bot პოლისები უნდა ადმინისტრირდებოდეს ცენტრალური კონსოლიდან.
- Anti-Virus და Anti-bot აპლიკაციას უნდა ქონდეს ცენტრალური მოვლენების კორელაციის და რეპორტინგის მექანიზმი.
- Anti-virus ფუნქციონალს უნდა შეეძლოს საფრთხის მატარებელ website-ებზე წვდომის პრევენცია.
- Anti-virus და Anti-bot ფუნქციონალს უნდა შეეძლოს SSL დაშიფრული ტრაფიკის ინსპექცია.
- Anti-Virus უნდა შეეძლოს დაარქივებული ფაილების სკანირება.
- გადაწყვეტილებას უნდა შეეძლოს C&C ტრაფიკის პატერნების ამოცნობა და დაბლოკვა.

ლოგირება - Logging

- ბრენდმაუერს უნდა ჰქონდეს ლოგირების ფუქნციონალი ლოკალურად, ცენტრალური მენეჯმენტის შემთხვევაში, უნდა შეიძლებოდეს ლოგების მართვის მოდულში ინტეგრაცია.
- შესაძლებელი უნდა იყოს ყველა უსაფრთხოების აპლიკაციის/ფუნქციონალის ლოგირება, შესაძლებელი უნდა იყოს მომხარებლების აქტივობების ლოგების განცალკევება მართვის აქტივობების ლოგებისგან.
- შესაძლებელი უნდა იყოს მოვლენების დახარისხება სხვადასხვა მახასიათებლის მიხედვით.
- ლოგირების ფუქნციონალს უნდა შეეძლოს შემდეგი ტიპის მოვლენების გენერაცია: Top sources, Top destinations, Top services, Top Actions, Top users, Top Origins, Top Firewall Rules.
- გადაწყვეტილებას უნდა შეეძლოს იგივე მწარმოებლის რეპორტინგის ცენტრალურ სისტემასთან (Reporting) ინტეგრაცია და გეგმიური რეპორტების დაგენერირება (ყოველდღიური, ყოველკვირეული და ყოველთვიური). მხარდაჭერილი უნდა იყოს არანაკლებ შემდეგი რეპორტინგის ფორმატები: HTML და PDF.

ცენტრალური მართვა, მოვლენების კორელაცია, რეპორტინგი - Policy Management, Reporting, Event Correlation

- შესაძლებელი უნდა იყოს ყველა ბრანდმაუერის ამავე მწარმოებლის ერთ მენეჯმენტ აპლიკაციასთან ინტეგრაცია.
- მენეჯმენტის აპლიკაციას უნდა შეეძლოს როლების და უფლებების მინიჭება ადმინისტრატორების ექაუნთების მიხედვით, მაგალითად: ადმინისტრატორს ჰქონდეს როლი და უფლება მხოლოდ პოლისების მართვის ან შეეძლოს მხოლოდ ლოგების დათვალიერება.
- ყველა უსაფრთხოების პოლიტიკის მართვა შესაძლებელი უნდა იყოს ცენტრალური კონსოლიდან.
- მართვის სისტემა უნდა მოიცავდეს ძებნის სწრაფ ინდექსირებულ ოფციას, რომლის საშუალებითაც შესაძლებელი იქნება მოიძებნოს უსაფრთხოების წესები რომლებიც მოიცავენ კონკრეტულ IP-ის ან მის ნაწილს.
- შესაძლებელი უნდა იყოს ცენტრალიზირებულად ახალი პროგრამული ვერსიების გავრცელება და დაყენება.
- შესაძლებელი უნდა იყოს ყველა შესაძლო ლიცენზიების ცენტრალიზირებულად მართვა.
- ლოგირების დათვალიერებისას შესაძლებელი უნდა იყოს ფილტრების დაყენება სხვადასხვა წინასწარ განსაზღვრული ობიექტებით (hosts, network, groups, users...)
- ბრენდმაუერს უნდა ჰქონდეს ხდომილებების კორელაციის საშუალება ჩაშენებული ან იმავე მწარმოებლის დამატებითი ცენტრალიზირებული პროგრამული უზრუნველყოფის საშუალებით.
- რეპორტინგ სისტემას უნდა შეეძლოს კონსოლიდირებული ინფორმაციის ჩვენება მართვის სისტემაში გაერთიანებული ყველა მოწყობილობიდან.

რისკებთან და სტანდარტებთან შესაბამისობა - Governance Compliance

- შესაძლებელი უნდა იყოს რისკების მართვისა და სტანდარტებთან შესაბამისობის (Compliance) ფუნქციონალის სრული ინტეგრაცია ბრენდმაუერის სისტემაში.
- შესაძლებელი უნდა იყოს რეალურ დროში შეამოწმდეს ძირითადი რეგულაციების (PCI DSS, HiPPA, SOX...) მიმართ შესაბამისობა
- შესაძლებელი უნდა იყოს პოლისის გააქტიურების დროს რეგულაციებთან შესაბამისობის დარღვევის შემთხვევაში მყისიერად მოხდეს შეტყობინება.
- ფუნქციონალი უნდა იძლეოდეს ქმედით რეკომენდაციებს თუ როგორ გაუმჯობესდეს რეგულაციების მიმართ შესაბამისობა
- შესაძლებელი უნდა იყოს ავტომატური შეფასების რეპორტების დაგენერირება ტოპ რეგულატორების მიმართ.
- ფუნქციონალი სრულად უნდა ინტეგრირდებოდეს ცენტრალურ სამართავ სისტემაში.

ტექნიკური მოთხოვნები მხარდაჭერილი ფუნქციონალის მიმართ

ამავე გადაწყვეტილებაში სამომავლოდ უნდა შეიძლებოდეს აღნიშნული ფუნქციონალის დამატება შესაბამისი ლიცენზიების განახლებით.

კიბერ-საფრთხეებისგან დაცვა - Advanced Sandboxing

- თანამედროვე კიბერ-საფრთხეებისგან დაცვისთვის, ამავე გადაწყვეტილებაში ლიცენზიის დამატებით უნდა შეიძლებოდეს Sandboxing ფუნქციონალის გააქტიურება.
- ახალი თაობის ბრანდმაუერი და Sandbox გადაწყვეტილება უნდა იყოს ერთი და იმავე მწარმოებლის.
- გადაწყვეტილებას უნდა შეეძლოს ე.წ "Zero-Day" ახალი თაობის უცნობი საფრთხეების პრევენცია.

- გადაწყვეტილებას უნდა შეეძლოს სრული ინტეგრაცია ამავე მწარმოებლის Cloud Sandbox-თან.
- მწარმოებლის Sandbox მხარდაჭერილი უნდა ჰქონდეს ინტეგრაცია ბრანდმაუერების მართვის ცენტრალურ სისტემასთან, მათ შორის, ცნეტრალურად პოლიტიკების მართვა, ლოგების ერთიანი მიღება, ანალიზი და რეპორტინგი.
- მწარმოებლის Sandbox გადაწყვეტილებას უნდა შეეძლოს გამშვები ფაილების (executable), არქივების, დოკუმენტების, JAVA და Flash გაფართოებების ემულაცია, მათ შორის: 7z, doc, docx, xlsx, pptx, pps, exe, jar, pdf, jar, rar, tar, tgz, ,zip, swf, scr.

სერვისები და საინსტალაციო სამუშაოები

- ბრანდმაუერის მწარმოებელი ვენდორისა და ინტეგრატორის ექსპერტების მიერ უნდა მოხდეს სისტემის დანერგვის გეგმის შემუშავება, რაც მოიცავს დამკვეთის არსებულ ქსელის ტოპოლოგიაში სისტემის იმპლემენტაციის შემდეგ გეგმას:
    - ბრანდმაუერის შასის ფიზიკური ინსტალაცია და უსაფრთხოების მოდულების აწყობა.
    - ოპერაციული სისტემის ინსტალაცია უსაფრთხოების შასის ყველა მოდულისთვის და პროგრამული განახლებების დაყენება.
    - დამკვეთის არსებული ბრანდმაუერის სისტემიდან კონფიგურაციის გადატანა ახალ სისტემაზე, მათ შორის უსაფრთხოების პოლიტიკების წესების.
    - ახალი სისტემებიდან კონფიგურაციების ბექაფების აღება და შენახვა.
    - ახალი სისტემის მონიტორინგი შესაძლო პრობლემების აღმოჩენისა და აღმოფხვრისთვის.
    - ვენდორისა ექსპერტის მიერ უნდა მოხდეს დამკვეთის გუნდისთვის ახალ სისტემაზე ცოდნის გადაცემა (knowledge transfer).

სსიპ განათლების მართვის საინფორმაციო სისტემა

უფროსი

დიმიტრი ბერიძე _____ ბ.ა.

შპს იუ ჯი თი

გენერალური დირექტორი

ერმილე სულაძე _____ ბ.ა.

საქართველოს ბანკი
ბიზნესი

ხელშეკრულების შესრულების საბანკო გარანტია # PE42993-18

თბილისი 07 აგვისტო 2018 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, ქ. თბილისის ვაკის რაიონში, ჭავჭავაძის გამზირი, №17ა
ბენეფიციარი: სსიპ განათლების მართვის საინფორმაციო სისტემა (შემდგომში „ბენეფიციარი")
ბენეფიციარის საიდენტიფიკაციო კოდი: 205300048
საგარანტიო თანხა: 14,917.50 (თოთხმეტი ათას ცხრაასჩვიდმეტი და 50/100) ლარი
ტენდერის უნიკალური ნომერი: #SPA180006286

მხედველობაში ვიღებთ რა, რომ პრინციპალმა უსაფრთხოების სისტემის მიწოდების (თანმდევი ინსტალაციით) 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 14,917.50 (თოთხმეტი ათას ცხრაასჩვიდმეტი და 50/100) ლარი და ვკისრულობთ ზემოთ აღნიშნული თანხის, გადახდას პრინციპალის მიერ ხელშეკრულების პირობების დარღვევის შემთხვევაში ბენეფიციარის წერილობითი მოთხოვნის წარმოდგენის საფუძველზე.

ბენეფიციარის წერილობითი მოთხოვნა თანხის ანაზღაურებაზე წარმოდგენილ უნდა იქნეს ბენეფიციარის მხრიდან აღნიშნული დოკუმენტზე უფლებამოსილი პირის მიერ ხელმოწერილი ფორმით, სადაც მითითებულ იქნება მოთხოვნილი თანხა ციფრობრივად და სიტყვიერად, საბანკო რეკვიზიტები და განმარტებული უნდა იყოს პრინციპალსა და ბენეფიციარს შორის გაფორმებული ხელშეკრულების რა პირობები იქნა დარღვეული პრინციპალის მხრიდან დამატებითი მტკიცებულებების წარმოდგენის აჭიროების 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: 30 იანვარი 2019 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 ფინანსირების დეპარტამენტის საყურადღებოდ, თბილისის დროით (UTC / GMT +04: 00 საათი) 17:00 საათის ჩათვლით, შემდეგ მისამართზე: გაგარინის ქ.#29ა, თბილისი 0160, საქართველო.

საბანკო გარანტია ავტომატურად უქმდება 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.

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,
ეთერ ბაქრაძე
გარანტიების სამსახურის უფროსი

სს „საქართველოს ბანკი"
საქართველო, თბილისი 0160
გაგარინის ქ. №29
www.corporate.ge
(0 32) 2 444 444