სს „ტერაბანკი“ **აცხადებს ტენდერს პროგრამული უზრუნველყოფის ინფორმაციის გადინების თავიდან აცილების “DLP” სისტემის შესყიდვასა და იმპლემენტაციაზე**

**ტენდერში მონაწილე კომპანიები უნდა აკმაყოფილებდნენ შემდეგ საკვალიფიკაციო მოთხოვნებს:**

* შესაბამის სფეროში სამუშაო გამოცდილება არანაკლებ 5 წელი;

**სატენდერო განაცხადი უნდა შეიცავდეს შემდეგ დოკუმენტაციას:**

* ფასი წარმოდგენილი უნდა იყოს საქართველოს კანონმდებლობით გათვალისწინებული ყველა გადასახადის ჩათვლით.
* კომპანიის კორპორატიული კლიენტების ჩამონათვალი, საკონტაქტო პირების მითითებით;
* ამონაწერს სამეწარმეო რეესტრიდან;
* ცნობას საგადასახადო ორგანადან დავალიანების არქონის შესახებ;
* შეთანხმებას კონფედენციალურობაზე, შევსებული (იხ. თანდართული ფაილი);
* საბანკო ამონაწერს ან ცნობას საბანკო ანგარიშებზე ბრუნვის შესახებ (6 თვის);

**ტენდერის აღწერილობა** **და მოთხოვნები:**

1.           პროგრამული უზრუნველყოფა უნდა მიეკუთვნებოდეს Enterprise DLP სისტემების კლასს და უნდა ჰქონდეს როგორც საბოლოო წერტილების კონფიდენციალური მონაცემების გადინებისაგან დაცვის ფუნქციონალი, რომელიც აგენტის საბოლოო წერტილებზე (EndPoint) ყენდება, ასევე კონფიდენციალური ინფორმაციის ქსელური არხების მეშვეობით გადინების კონტროლის ფუნქციონალი (Network DLP) და ელ-ფოსტის ტრაფიკის კონტროლის ფუნქციონალი განიხილება დადებითად.

2.            პროგრამული უზრუნველყოფა უნდა წარმოადგენდეს კონფიდენციალური მონაცემების გადინების თავიდან აცილების სისტემების ბაზრის ერთ-ერთ ლიდერს  სააგენტო Gartner-ის  კლასიფიკაციის მიხედვით.

3.            პროგრამული უზრუნველყოფის კომერციული წინადადება უნდა შეიცავდეს კონფიდენციალური მონაცემების გადინებისაგან საბოლოო წერტილების დაცვის ფუნქციონალს.

4.            შეთავაზებული პროგრამული  უზრუნველყოფა უნდა უზრუნველყოფდეს შემდეგ მოთხოვნებს:

4.1.        საბოლოო წერტილების დაცვა კონფიდენციალური მონაცემების გადინებისგან, კონფიდენციალური მონაცემების გამოვლენა საბოლოო წერტილებზე, მონაცემების კლასიფიკაცია და მიზანმიმართული შეტევებისგან დაცვა, ქსელურ დისკებსა და ღრუბლოვან სივრცეებში კლასიფიცირებული მონამეცემების ძებნა და დაცვა..

4.2.        უზრუნველყოს საოპერაციო სისტემა: Windows (Desktop/Server), Linux (Desktop/Server – Red Hat Enterprise Linux, Debian Linux, Suse Linux, Ubuntu Linux), Mac OSX (Desktop/Server) მართვის ქვეშ მომუშავე საბოლოო წერტილების დაცვა.

4.3.        უზრუნველყოფდეს Virtual Desktop Infrastructure საოპერაციო სისტემის ქვეშ მომუშავე საბოლოო წერტილების დაცვას.

4.4.        უზრუნველყოს კონფიდენციალური მონაცემების გამოვლენა ყველა საბოლოო წერტილში, რომლებიც მუშაობენ საოპერაციო სისტემა: Windows (Desktop/Server), Linux (Desktop/Server), Mac OSX (Desktop/Server) მართვის ქვეშ, მონაცემთა ბაზებში, Share Point-ში, file shares -ში (Windows,Samba,CIFS,NFS).

4.5.        კონფიდენციალური მონაცემების გამოვლენის მექანიზმი უნდა უზრუნველყოფდეს ინფორმაციის იდენტიფიკაციის შემდეგ მეთოდებს:

4.5.1.     სტრიქონების, საკვანძო სიტყვების, რეგულარული გამოთქმების, ლექსიკონების მიხედვით;

4.5.2.     მონაცემთა ციფრული ანაბეჭდების მიხედვით;

4.5.3.     კონტექსტური კლასიფიკაციის მიხედვით;

4.5.4.     მონაცემთა ზუსტი და სრული დამთხვევის მიხედვით.

4.6.        უზრუნველყოს კონფიდენციალური მონაცემების დაცვა გადინებისგან ღრუბლოვან სერვისებში (ლიცენზია ამ ფუნქციონალზე ამ ეტაპზე არ უნდა შედიოდეს კომერციულ წინადადებაში, მაგრამ შეთავაზებული პროგრამული უზრუნველყოფა უნდა იყენებდეს ამ  ფუნქციონალს მასშტაბირების ხარჯზე მომავალში შესაბამისი სერვისის შეძენის გზით).

4.7.        აკონტროლოს კონფიდენციალური მონაცემების გამოყენება საბოლოო წერტილებზე მომუშავე ნებისმიერი პროგრამის  – საფოსტო კლიენტების, web-ბრაუზერების, საოფისე აპლიკაციების, Acrobat, Instant Messengers მიერ და ა.შ.

4.8.        უზრუნველყოს Copy, Move, Save As,  Open, Close, Read, Write, and Edit-ის ფაილებთან ოპერაციების კონტროლი  საბოლოო წერტილებზე კონფიდენციალური მონაცემების გადინების თავიდან აცილებისთვის.

4.9.        აკონტროლოს საბოლოო წერტილებიდან კონფიდენციალური მონაცემების ატვირთვა ქსელში, ღრუბლოვან სერვისებსა და ინტერნეტში.

4.10.     აკონტროლოს კონფიდენციალური მონაცემების ბეჭდვა.

4.11.     აკონტროლოს კონფიდენციალური მონაცემების გაცვლა სხვადასხვა პროგრამებს შორის საბოლოო წერტილებზე, რომელთა რეალიზაცია ხდება  Cut, Copy, Paste, Insert, PrintScreen ბრძანებების მეშვეობით.

4.12.     აკონტროლოს კონფიდენციალური მონაცემების გადატანა სხვადასხვა გარე მატარებლების მეშვეობით (CD/DVD, ფლეშ მეხსიერების ბარათები, გარე ვინჩესტერები) და პოლიტიკების მიხედვით ჰქონდეს კონფიდენციალური მონაცემების კოპირების ოპერაციების ბლოკირების შესაძლებლობა.

4.13.      საბოლოო წერტილებზე დასაყენებელ აგენტს უნდა ჰქონდეს (საჭიროების შემთხვევაში) მომხმარებლისათვის  «უხილავ» რეჟიმში მუშაობის შესაძლებლობა.

4.14.      საბოლოო წერტილებზე დასაყენებელი აგენტის წაშლა შესაბამისი ავტორიზაციის გარეშე გამორიცხული უნდა იყოს საბოლოო წერტილზე ადმინისტრატორული პრივილეგიების არსებობის შემთხვევაშიც კი.

4.15.      აკონტროლოს სხვადასხვა DLL-ბიბლიოთეკების გამოძახება პროგრამების მეშვეობით საბოლოო წერტილებზე და დაბლოკოს ეს გამოძახებები უსაფრთხოების პოლიტიკის დარღვევის რისკის წარმოქმნის შემთხვევაში.

4.16.     აკონტროლოს სხვადასხვა პროგრამების გაშვება საბოლოო წერტილებზე და დაბლოკოს ეს გაშვებები ინფორმაციული უსაფრთოხების პოლიტიკის დარღვევის რისკის წარმოქმნის შემთხვევაში.

4.17.      უზრუნველყოს პროგრამების ინვენტარიზაცია საბოლოო წერტილებზე.

4.18.      უზრუნველყოფდეს Microsoft Active Directory-სთან ინტეგრაცია.

4.19.      უზრუნველყოს მონაცემთა კლასიფიკაციის შემდეგი მეთოდები:

4.19.1.  ავტომატური, დაფუძნებული კონტექსტზე  (მაგალითად, კონფიდენციალური მონაცემების შემცველი ფაილის ადგილმდებარეობის შესახებ ინფორმაციის საფუძველზე).

4.19.2.  ავტომატური, დაფუძნებული კონტენტზე (ფაილის შინაარსზე/e-mail)

4.19.3.  ავტომატური, დაფუძნებული საფაილე ოპერაციებზე (კლასიფიკაციის ტეგი განისაზღვრება ფაილის გადაადგილების მარშრუტით ან e-mail).

4.19.4.  ავტომატური, რომელიც განისაზღვრება აპლიკაციით (კლასიფიკაციის ტეგი განისაზღვრება აპლიკაციით, რომელიც   ქმნის/მოდიფიცირებას უკეთებს ფაილს).

4.19.5.  ავტომატური, რომელიც განისაზღვრება ფაილის/e-mail-ის მომხმარებლისათვის/მომხმარებელთა ჯგუფისათვის კუთვნილებით.

4.20.      უზრუნველყოფდეს ფაილების/e-mail-ის ტეგირება:

4.20.1.  კლასიფიკაციის შედეგი უნდა გაფორმდეს ტეგის სახით.

4.20.2.  ტეგი უნდა შეინახებოდეს ფაილებთან/e-mail-თან მანიპულაციების მიუხედავად.

4.20.3.  მინიჭებული ტეგი უნდა გადადიოდეს მემკვიდრეობით.

4.20.4.  უზრუნველყოფილი უნდა იყოს ტეგების სიმრავლე, რომელიც ერთი და იგივე ფაილის/e-mail-ის მიმართ გამოყენებული კლასიფიკაციის სხვადასხვა მეთოდების შედეგს ასახავს.

4.20.5.  ტეგები უნდა იყოს ხილული ფაილების არქივაციის შემთხვევაშიც კი (მაგალითად,  ZIP/RAR-ფორმატში).

4.21.      უზრუნველყოფდეს SIEM/Log Management-ის სისტემებთან ინტეგრაციას.

4.22.     პოტენციურმა ორგანიზაცია-შემსრულებელმა უნდა წარადგინოს MAF-ი შესაბამისი  პროგრამული უზრუნველყოფის «ინფორმაციის გადინების თავიდან  აცილების სისტემის» გაყიდვის უფლებაზე.

4.23.      პოტენციურ ორგანიზაციას-შემსრულებელს უნდა ჰქონდეს შესაბამისი პროგრამული უზრუნველყოფის  «ინფორმაციის გადინების თავიდან  აცილების სისტემის» ქვეყანაში მიწოდების გამოცდილება.

4.24.      იმპლემენტაცია უნდა განხორციელდეს ან ორგანიზაციის-შემსრულებლის სერტიფიცირებული სპეციალისტების მიერ, ან მწარმოებლის ინჟინრების მიერ ან ერთისა და მეორის მიერ.

**აუცილებელი პირობა:**

* მომსახურე კომპანიასთან ანგარიშწორება განხორციელდება მხოლოდ სს „ტერაბანკ“-ში გახსნილი საბანკო ანგარიშის საშუალებით.
* სატენდერო წინადადება წარმოდგენილი უნდა იყოს სს „ტერაბანკი“-ს კანცელარიაში: მისამართი: თბილისი, წმ ქეთევან დედოფლის გამზ.#3.

**კონვერტზე მითითებული უნდა იყოს შემდეგი მონაცემები:**

* კომპანიის დასახელება;
* საკონტაქტო ინფორმაცია (საკონტაქტო პირი, მობ.ნომერი/ტელეფონი, ელ-ფოსტა; მისამართი);
* ტენდერის დასახელება – „ტენდერს პროგრამული უზრუნველყოფის  «ინფორმაციის გადინების თავიდან  აცილების DLP სისტემის» შესყიდვასა და იმპლემენტაციაზე “
* ხელმოწერა და კომპანიის ბეჭედი კონვერტის დალუქვის ადგილზე;

|  |
| --- |
| სატენდერო წინადადების წარმოდგენის ბოლო ვადაა **2019 წლის 2 სექტემბერი (18:00 სთ-მდე)**. |

ტექნიკურ საკითხთან დაკავშირებით დაუკავშირდით გიორგი ხუციშვილს, ელ. ფოსტის შემდეგ მისამართზე: Giorgi.Khutsishvili@terabank.ge ტელეფონზე 255 00 00 / (შიდა 1160). მობ: 595 957888

სხვა ტენდერთან დაკავშირებულ კითხვებზე დაუკავშირდით ირაკლი მიქაძეს, ფოსტის შემდეგ მისამართზე: [Irakli.mikadze@terabank.ge](mailto:Irakli.mikadze@terabank.ge) , ტელეფონზე 255 00 00 / (შიდა 2005). მობ: 595 60 01 04

**შენიშვნა:** ბანკი იტოვებს უფლებას არ განიხილოს შემოსული წინადადება, რომელშიც არასრულად იქნება წარმოდგენილი მოთხოვნილი დოკუმენტაცია.