ტექნიკური დავალება

ელექტრონული ფოსტის უსაფრთხოების პროგრამული პაკეტი
(Email Security Gateway)

1. გადაწყვეტილების ტიპი	***ვირტუალური მოწყობილობა***
2. ლიცენზიის ვადა	3 წელი
3. თავსებადობა ვირტუალიზაციის პლატფორმებთან	VMware ESXi 5.5/6.0/6.5 და ზემოთ
4. მწარმოებლის გამოცდილება	არანაკლებ 5 წლიანი გამოცდილება ელექტრონული ფოსტის უსაფრთხოების გადაწყვეტილებათა (Email Security Gateway) წარმოებაში
5. მწარმოებლის მხარდაჭერა	შემოთავაზებულ პროდუქტზე უნდა ვრცელდებოდეს მწარმოებლის 3 (სამი) წლიანი საგარანტიო მომსახურება, ტექნიკური მხარდაჭერა, პროგრამული უზრუნველყოფის, სიგნატურების განახლების, რეპუტაციული ბაზების განახლების სერვისი
6. მხარდაჭერის პირობები	სატელეფონო, ელექტრონული ფოსტის, ონლაინ ჩატისა და Ticket სისტემის მეშვეობით - 24/7
7. ლიცენზიის ვადის გასვლა	შემოთავაზებული პროდუქტის ლიცენზიის ვადის გასვლისას ძირითადი სერვისები ავტომატურად არ უნდა გაჩერდეს და უნდა განაგრძოს მუშაობა ჩვეულ რეჟიმში - perpetual license-ის მქონე პროგრამული უზრუნველყოფების მსგავსად, მხოლოდ ე.წ. subscription-ების, upgrade-ებისა და signature-ების განახლების სერვისის გაჩერებით და მათი შემდგომი შესყიდვის შესაძლებლობით.
8. პრეტენდენტის ავტორიზაცია	პრეტენდენტმა უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturers Authorization Form)
9. პრეტენდენტის ინჟინერი	პრეტენდენტს უნდა ჰყავდეს დასაქმებული მწარმოებლის მიერ სერტიფიცირებული ადგილობრივი ქართულენოვანი ინჟინერი და წარმოადგინოს შესაბამისი სერტიფიკატი.
10. პრეტენდენტის გამოცდილება	ბოლო სამი წლის განმავლობაში პრეტენდენტს უნდა ჰქონდეს შემოთავაზებული პროდუქტის არანაკლებ ორჯერ მაინც წარმატებული დანერგვის გამოცდილება საქართველოში და წარმოადგინოს შესაბამისი ხელშეკრულებები და მიღება-ჩაბარების აქტები
11. დანერგვა	პრეტენდენტმა უნდა უზრუნველყოს შემოთავაზებული პროდუქტის სახელმწიფო აუდიტის სამსახურის სისტემაში საჭირო საკონფიგურაციო სამუშაოების ჩატარება და პროდუქტის სრული დანერგვა
12. მოწოდება-დანერგვის ვადები	12.1 მოწოდების ვადა - ხელშეკრულების გაფორმებიდან არაუგვიანეს 10 სამუშაო დღისა 12.2 დანერგვა - კონფიგურაცია - მოწოდებიდან არაუგვიანეს 20 სამუშაო დღისა
13. წარმადობა	13.1 გამტარუნარიანობის მოცულობა (წერილი/საათში) - არანაკლებ 67 000; 13.2 ანტისპამის გამტარუნარიანობა (წერილი /საათში) - არანაკლებ 54 000; 13.3 ანტისპამის + ანტივირუსის გამტარუნარიანობა (წერილი/საათში) - არანაკლებ 52 000; 13.4 დომენების რაოდენობა – არანაკლებ 100;

	13.5 საფოსტო ყუთების რაოდენობა სერვერულ რეჟიმში – არანაკლებ 400; 13.6 დაცვის პოლიტიკების რაოდენობა (დომენი/სისტემა): 400 /1 500; 13.7 უსაფრთხოების პროფილის რაოდენობა (დომენი/სისტემა): 50/200.
14. ქსელური ტექნოლოგიები და სერვისები	14.1 მუშაობის რეჟიმები: Transparent, Gateway, Mail Server; 14.2 შემავალი და გამავალი ტრაფიკის ინსპექტირება; 14.3 IPv4 და IPv6 მხარდაჭერა; 14.4 მოქნილი ელ. ფოსტის ინსპექტირების პოლიტიკები (ცალკე დაცული და დაუცველი დომენებისთვის, IP მისამართების, გამგზავნი და მიმღების მონაცემების მიხედვით); 14.5 საფოსტო პროტოკოლების მოქნილი პროფილები: მათი შეზღუდვის შესაძლებლობა, RFC მოთხოვნების შემოწმება, პაკეტების თავსართის გამოყენების შესაძლებლობა; 14.6 SMTP ავთენტიფიკაციის მხარდაჭერა: LDAP, RADIUS, POP3, and IMAP; 14.7 ელ ფოსტის მარშრუტიზაცია LDAP. ელ ფოსტის ინსპექცია LDAP ატრიბუტების გამოყენებით პოლიტიკის (დომენის) მიხედვით; 14.8 გეოლოკაციის მხარდაჭერა ელ. ფოსტის ინსპექტირების პოლიტიკებში; 14.9 ელ. ფოსტის რიგის მართვა; 14.10 ფოსტის არქივაცია ცალკე შენახვის შესაძლებლობით; 14.11 ვებფოსტის მომხმარებლის ინტერფეისი, სერვერის რეჟიმში მუშაობის შემთხვევაში; 14.12 ლოკალური მომხმარებლების მონაცემთა ბაზის მხარდაჭერა სერვერის რეჟიმში მუშაობის შემთხვევაში; 14.13 მავნე შინაარსის შეტყობინების დამოუკიდებლად ჩანაცვლების შესაძლებლობა; 14.14 რამდენიმე სერვერს შორის ელ. ფოსტის ტრაფიკის ბალანსირების მექანიზმის მხარდაჭერა; 14.15 მოქნილი სარეზერვო ასლების წარმოება: ელ. ფოსტის, სისტემური და მომხმარებლის კონფიგურაციის სარეზერვო ასლების ავტომატური შექმნა;
15. დაცვის მექანიზმები	15.1 ანტისპამი: 15.1.1 გლობალური რეპუტაციული გამგზავნის ბაზა/ გამგზავნების გლობალური რეპურაციული ბაზა; 15.1.2 ელ. წერილების შემოწმება საკონტროლო ჯამურ მაჩვენებელზე (checksums); 15.1.3 დინამიური ევრისტიკული ანალიზის წესების მიღება; 15.1.4 სპამისგან დაცვა (spam outbreak); 15.1.5 ლოკალური მისამართების და მისამართების რეპუტაციული სიის მხარდაჭერა; 15.1.6 ფოსტის Antispoofing (ცრუ მისამართების საწინააღმდეგო), საკუთარი დომენის დაცვა უკანონო გამოყენებისგან. სათაურის შედარების სავალდებულო არჩევანის საშუალება From: envelope sender ან Reply-To: address 15.1.7 სპამის აღმოსაჩენად ქცევითი ანალიზის გამოყენება; 15.1.8 ელ. ფოსტის თავსართის ღრმა ანალიზი; 15.1.9 უსაფრთხოების სხვადასხვა ინციდენტის დროს სისტემის ქმედების მოქნილი პროფილის შექმნის შესაძლებლობა; 15.1.10 სხვა ვენდორების მოწყობილობებიდან URLs-ების შავი სიის გამოყენების შესაძლებლობა (SURBL/RBL) 15.1.11 სხვა ვენდორების მოწყობილობებიდან IP მისამართების და DNS IP (DNSBL) შავი სიის მხარდაჭერა 15.1.12 PDF სკანირების და სურათის ანალიზი; 15.1.13 შავი და თეთრი სიის გლობალურად, დომენის დონეზე და მორგებულად შექმნის შესაძლებლობა;

	15.1.14 Bayes სტატიკური ფილტრაცია; 15.1.15 SPF, DKIM, DMARC შემოწმების სტანდარტის მხარდაჭერა; 15.2 ანტივირუსი: 15.2.1 წერილების და მიმაგრებული ფაილების სიგნატურული და ევრისტიკული ანალიზი; 15.2.2 წინასწარი დაცვა მავნე პროგრამების გავრცელებისგან (virus outbreak); 15.2.3 დამატებითი ე.წ. „grayware“ აღმოჩენა; 15.2.4 სხვადასხვა სახის მავნე პროგრამების გამოვლენის პროფილების შექმნის შესაძლებლობა; 15.3 DLP და შინაარსის ფილტრაცია: 15.3.1 ფაილების ანაბეჭდის შექმნა და მათი გაგზავნის ბლოკირება; 15.3.2 კონფიდენციალური ინფორმაციის აღმოჩენა და დაბლოკვა; 15.3.3 შინაარსის ფილტრაცია HIPAA, SOX, GLBA ლექსიკონების ან საკუთარი ფრაზების მიხედვით; 15.3.4 მიბმული ფაილების ფილტრაცია შინაარსის ან გაფართოების მიხედვით; 15.3.5 დაშიფრული არქივების/PDF/Office ავტომატური შემოწმება, ასევე პაროლების სიის გამოყენება; 15.3.6 მავნე კოდის ან ბმულების წაშლის შესაძლებლობა PDF, Microsoft Office ფაილებიდან ორიგინალის შეცვლის გარეშე; 15.4 დამატებითი უსაფრთხოების ტექნოლოგიები: 15.4.1 გამგზავნის გადამოწმების მექანიზმები (Spoof- ისგან დაცვა, გაყალბების ანალიზი); 15.4.2 Url გადამოწმების მექანიზმი წერილებში (URL Click Protection); 15.4.3 სისტემის ინტეგრირების შესაძლებლობა სხვა ინდივიდუალურ მოწყობილობებთან, როგორიცაა Firewall, Sandbox და ა.შ. 15.4.4 მავნე ან აკრძალული შინაარსის მქონე წერილების კარანტინში მოთავსება და სისტემურ ადმინისტრატორისთვის მოვლენის შესახებ შეტყობინებების გაგზავნა 15.4.5 ფოსტის შიგთავსში ან თემაში საკვანძო სიტყვით ელექტრონული ფოსტის ბლოკირების შესაძლებლობა
16. შიფრაცია	16.1 სერვერიდან სერვერზე დაშიფვრის მოწინავე ალგორითმი და გასაღებების გაცვლა, დაშიფვრის ალგორითმები და ა.შ. TLS პარამეტრები; 16.2 S-MIME მხარდაჭერა; 16.3 HTTPS, SMTPS, SSH, IMAPS, POP3S მხარდაჭერა; 16.4 IBE შიფრაციის მხარდაჭერა;
17. თვითსწავლის რეჟიმი	შემოთავაზებულ სისტემას უნდა ჰქონდეს თვითსწავლის რეჟიმის გააქტიურებისა და უსაფრთხოების წესების ავტომატური შექმნის შესაძლებლობა. ასევე, უნდა ჰქონდეს წინასწარ ჩაშენებული სტანდარტული უსაფრთხოების პოლიტიკების შაბლონები.
18. მართვა, ლოგირება და რეპორტები	18.1 ცენტრალიზებული მართვის სისტემა - ვებ ინტერფეისი 18.2 როლებზე დაფუძნებული ადმინისტრაციული ანგარიშები; 18.3 სისტემას უნდა შეეძლოს, მოთხოვნისამებრ რეპორტების გენერირება. რეპორტების გენერირება ასევე შესაძლებელი უნდა იყოს წინასწარ განსაზღვრული გრაფიკის მიხედვით 18.4 TCP კავშირების მონიტორინგი, ელ. ფოსტის შეტყობინებები და უსაფრთხოების მოვლენები რეალურ დროში; 18.5 ლოგირების სისტემის ცვლილებები და უსაფრთხოების ინციდენტები; 18.6 ჩაშენებული რეპორტინგების მოდულები; 18.7 ცენტრალიზებული შესვლის და რეპორტინგის შესაძლებლობა დამატებული სპეციალიზებული მოწყობილობების შემთხვევაში; 18.8 SNMP მხარდაჭერა; 18.9 Syslog პროტოკოლის მხარდაჭერა; 18.10 ელ. წერილები კატეგორიის და მოვლენის მიხედვით.

შენიშვნა:

წარმოდგენილი დოკუმენტი უნდა დადასტურდეს მომწოდებლის მიერ კვალიფიციური ელექტრონული ხელმოწერით ან/და კვალიფიციური ელექტრონული შტამპით.