**(DLP) Data Loss Prevention გადაწყვეტილების ტექნიკური დავალება**

1. **ფუნქციონალური მოთხოვნები:**

1.1. შემოთავაზებულ გადაწყვეტილებას უნდა ჰქონდეს ფუნქციონალი, რომელიც უზრუნველყოფს კონფიდენციალური მონაცემების გაჟონვისგან დაცვას ბოლო წერტილებზე დაინსტალირებული აგენტის (EndPoint DLP) გამოყენებით და კონფიდენციალური მონაცემების გაჟონვის კონტროლის ფუნქციონალს ქსელური არხების (Network DLP) მეშვეობით.

1.2. შემოთავაზებულმა გადაწყვეტილებამ უნდა უზრუნველყოს სამუშაო სადგურებსა და ფაილ სერვერებზე განთავსებული კონფიდენციალური ინფორმაციის მოძიების შესაძლებლობა (ნაპოვნი ფაილების კარანტინში გადატანისა და ასეთი ფაილების ადგილზე დატოვების შესაძლებლობით).

1.3. შემოთავაზებულმა გადაწყვეტილებამ უნდა აკონტროლოს კონფიდენციალური ინფორმაციის პოტენციური გაჟონვის შემდეგი არხები:

* გამავალი SMTP კავშირები;
* გამავალი HTTP კავშირები;
* გამავალი HTTPS კავშირები;
* FTP, SFTP
* გამავალი IM კავშირები;
* ინფორმაციის კოპირება გარე შენახვის მედიასა და საინფორმაციო რესურსებზე;
* ინფორმაციის ბეჭდვა ლოკალურ/ქსელურ პრინტერზე.
* Screenshot

1.4. შემოთავაზებულმა გადაწყვეტილებამ უნდა უზრუნველყოს შემდეგი ფუნქციური შესაძლებლობები:

* კონფიდენციალური ინფორმაციის გამჟღავნების თავიდან აცილება კორპორატიული საფოსტო სისტემის მეშვეობით;
* კონფიდენციალური ინფორმაციის შემცველი გამავალი ელფოსტის დაბლოკვის შესაძლებლობა;
* კონფიდენციალური ინფორმაციის გამჟღავნების თავიდან აცილება კორპორატიული ინტერნეტ წვდომის სისტემის მეშვეობით;
* კონფიდენციალური ინფორმაციის HTTP/HTTPS ტრაფიკიდან ამოღების შესაძლებლობა;
* HTTP/HTTPS ტრაფიკის დაბლოკვის შესაძლებლობა;
* კონფიდენციალური ინფორმაციის გამჟღავნების თავიდან აცილება და გაჟონვის არხების მონიტორინგი, კერძოდ: კონფიდენციალური ინფორმაციის კოპირება ქსელური საქაღალდიდან ლოკალურ მყარ დისკებზე, კონფიდენციალური ინფორმაციის კოპირება მოსახსნელ მედიაზე, კონფიდენციალური ინფორმაციის გაგზავნა ლოკალურ და ქსელურ ბეჭდვაზე, ასევე ფაქსით, ბუფერული მეხსიერების შიგთავსის დაცვა კოპირება/ჩასმის ოპერაციების დროს;
* კონფიდენციალური ინფორმაციის სკანირების (მათ შორის, მითითებული გრაფიკით) შესაძლებლობა საბოლოო წერტილების ლოკალური მყარი დისკების სკანირებისა და ნაპოვნი ფაილების გადატანის შესაძლებლობით;
* გრაფიკულ ობიექტებში (pdf ფაილები, სურათები და ა.შ.) შემავალი ტექსტური ინფორმაციის, ასევე ასეთ ობიექტებში არსებული გრაფიკული სურათების (პასუხისმგებლიანი პირების ხელმოწერები, მარკები, ლოგოები და ა.შ.) ამოცნობის უნარი;
* კონფიდენციალური მონაცემების სკანირების და მათგან „ციფრული თითის ანაბეჭდების“ აღების შესაძლებლობა, ხოლო დაცული მონაცემების შესაბამისობის ზომის მინიმალური ზღვარი (ჰეშ ჯამი), რომელიც იწვევს უსაფრთხოების მოვლენას, უნდა იყოს 64 ბაიტიდან, ზღვარი კი 128 ბაიტიდან;
* მოწოდებულ კონფიდენციალურ დოკუმენტებზე თვითსწავლის შესაძლებლობა, მსგავსი დოკუმენტების შემდგომი დაბლოკვით;
* კლიენტებისა და პროგრამული მოდულების (აღმოჩენის სერვერების) ავტონომიურად მართვის შესაძლებლობა, კორპორატიული ქსელიდან საბოლოო წერტილის გათიშვის ან ქსელთან კავშირის დაკარგვის შემთხვევაში;
* უსაფრთხოების პოლიტიკის ცენტრალიზებული ადმინისტრირების შესაძლებლობა;
* უსაფრთხოების პოლიტიკაში რეალურ დროში ცვლილებების სწრაფად შეტანის, არსებული წესების, პარამეტრების შეცვლის და ახალი წესების, პარამეტრების დამატების შესაძლებლობა;
* უსაფრთხოების პოლიტიკის დარღვევების შესახებ ავტომატური შეტყობინებების დაყენება;
* უსაფრთხოების პოლიტიკის დარღვევებზე რეაგირების სხვადასხვა ვარიანტების დაყენება;
* უსაფრთხოების პოლიტიკის დარღვევების თარიღებისა და ფაქტების შესახებ ანგარიშების დაყენება და გენერირება;
* მართვის კონსოლში ავტორიზაციისთვის არსებული Active Directory ანგარიშების გამოყენების შესაძლებლობა;
* AD ანგარიშის ატრიბუტების (სახელი, ტელეფონის ნომერი, განყოფილება, პოზიცია და ა.შ.) პირდაპირ გადაწყვეტილების მართვის კონსოლიდან ნახვის შესაძლებლობა

1. **ტექნიკური მოთხოვნები:**

2.1 შემდეგი ოპერაციების კონტროლის შესაძლებლობა:

* კონფიდენციალური ინფორმაციის ჩაწერა მოსახსნელ მედიაზე (USB, CompactFlash, SD);
* კონფიდენციალური ინფორმაციის ბეჭდვა (ქსელის და ლოკალურ პრინტერებზე);
* კონფიდენციალური ინფორმაციის კოპირება ბუფერში;
* კონფიდენციალური ინფორმაციის ჩაწერა ლოკალურ დისკებზე;
* კონფიდენციალური ინფორმაციის ჩაწერა CD / DVD-ზე;
* აპლიკაციების მიერ კონფიდენციალურ ინფორმაციაზე წვდომის შემთხვევები (მათ შორის, კონფიდენციალური ინფორმაციის შემცველი ფაილების გადატანა Teams-ის საშუალებით);
* კონფიდენციალური ინფორმაციის გაგზავნა HTTP პროტოკოლის მეშვეობით;
* კონფიდენციალური ინფორმაციის გაგზავნა HTTPS პროტოკოლის მეშვეობით;
* კონფიდენციალური ინფორმაციის გაგზავნა Web-mail პროტოკოლის მეშვეობით;
* კონფიდენციალური ინფორმაციის გაგზავნა SMTP პროტოკოლის მეშვეობით (ელ. ფოსტის კლიენტების მეშვეობით);
* კონფიდენციალური ფაილის ინფორმაციის კოპირება ქსელურ რესურსებზე, მათ შორის Office 365 რესურსებსა და სერვისებზე;
* Print Screen ფუნქციის გამოძახება საბოლოო წერტილის დონეზე;
* დოკუმენტების მასობრივი კოპირების შემთხვევები გარე მედიაზე (გადაწყვეტილებამ უნდა აკონტროლოს ფაილების რაოდენობა, რომელთა კოპირებაც მომხმარებელს შეუძლია გარე მედიაზე გარკვეული პერიოდის განმავლობაში);
* დოკუმენტების დაშიფვრის შესაძლებლობა გარე მედიაზე კოპირებისას. პაროლის დაყენების შესაძლებლობა როგორც მომხმარებლებისთვის, ასევე გადაწყვეტილების ადმინისტრატორისთვის;
* MTP პროტოკოლის დაბლოკვის შესაძლებლობა (კონტროლი გულისხმობს როგორც კონფიდენციალური ინფორმაციის გაჟონვის აღმოჩენის, ასევე კონფიდენციალური ინფორმაციის გადაცემის დაბლოკვის შესაძლებლობას (მითითებული პოლიტიკის შესაბამისად)

2.2. Windows-სა და Linux ოპერაციულ სისტემაზე ყველა დეტექციის მოდულის განლაგების შესაძლებლობა..

2.3. კონფიდენციალური ინფორმაციის გაჟონვაზე შემდეგი ტიპის რეაგირების შესაძლებლობა: ინფორმაციის პასუხისმგებელი პირის ან მფლობელისთვის ავტომატური შეტყობინება, ელექტრონული ფოსტით გაგზავნის დაბლოკვა, ვებ ფორმების საშუალებით მონაცემების გაგზავნის დაბლოკვა, სკრიპტის შესრულება, კონფიდენციალური ინფორმაციის წაშლა.

2.4. ინციდენტის ესკალაციისა და დამატებითი ქმედებების დაწყების შესაძლებლობა (მაგალითად, მგრძნობიარე ინფორმაციის დაშიფვრა, მგრძნობიარე ინფორმაციის გადატანა და ა.შ.).

2.5. ოპტიკური სიმბოლოების ამოცნობის შესაძლებლობა (OCR - ოპტიკური სიმბოლოების ამოცნობა) უნდა იყოს უზრუნველყოფილი ჩაშენებული ტექნოლოგიით/მექანიზმით, დამატებითი მესამე მხარის პროგრამული უზრუნველყოფის გამოყენების გარეშე, OCR ფუნქციონალი უნდა იყოს გადაწყვეტილების აგენტის ფუნქციონალის ნაწილი. გარდა ამისა, OCR  უნდა უზრუნველყოს ქართული ენის მხარდაჭერა.

2.6 ამოცნობის სისტემამ უნდა უზრუნველყოს შემდეგი ფაილის ფორმატების მხარდაჭერა:PDF, BMP, JPEG, PNG, TIFF.

2.7 ამოცნობის სისტემა უნდა ამოქმედდეს შემდეგ შემთხვევებში:

* დოკუმენტების ლოკალური სკანირება;
* კონფიდენციალური ინფორმაციის გარე მედიაზე კოპირება;
* კონფიდენციალური ინფორმაციის ფაილ სერვერზე კოპირება;
* კონფიდენციალური ინფორმაციის გაგზავნა HTTP / HTTPS-ის საშუალებით;
* კონფიდენციალური ინფორმაციის გაგზავნა Webmail პროტოკოლის მეშვეობით;
* კონფიდენციალური ინფორმაციის გაგზავნა SMTP პროტოკოლის მეშვეობით.

2.8. USB-ზე მომხმარებლის წვდომის დონის რეგულირების შესაძლებლობა.

2.9. „მოსვენების მდგომარეობაში“ მყოფი კონფიდენციალური ინფორმაციის იდენტიფიცირების შესაძლებლობა;

2.10 ადმინისტრატორისთვის პროაქტიული ინფორმირების შესაძლებლობა, როდესაც მომხმარებელი კომპიუტერში არასანდო USB დისკს ჩადებს;

2.11. გადაწყვეტილების აგენტის ფარულ რეჟიმში მუშაობის მხარდაჭერის შესაძლებლობა, რომელშიც ყყველა პროცესი უნდა იყოს დამალული საბოლოო მომხმარებლისგან.

2.12 შემოთავაზებული გადაწყვეტილება უნდა მოიცავდეს კონფიდენციალური ინფორმაციის შემცველი ფაილებისა და მონაცემთა ბაზების ციფრული ანაბეჭდების აღების ფუნქციონალურობას. შესაძლებელი უნდა იყოს შეუვსებელი დოკუმენტის ციფრული ანაბეჭდის შექმნა უკვე შევსებული დოკუმენტის გაჟონვის შემდგომი აღმოჩენის მიზნით. ციფრული ანაბეჭდების გამოყენება შესაძლებელია გადაწყვეტილების თითოეული კომპონენტის მიერ: საბოლოო წერტილზე განთავსებული აგენტის, კონფიდენციალური ინფორმაციის აღმოჩენის სერვერის ან ქსელის გაჟონვის პრევენციის კომპონენტის მიერ.

2.13 გადაწყვეტილებას უნდა ჰქონდეს რეალურ დროში ლოკალური მონიტორინგის შესაძლებლობა: შექმნილი, რედაქტირებული, გადმოწერილი ან ლოკალურ დისკზე კოპირებული ფაილის დაუყოვნებლივი სკანირების შესაძლებლობა შემდეგი მოქმედებებით: პოლიტიკის დარღვევების ჟურნალირება, ფაილის კოპირება, ფაილის გადატანა ადმინისტრატორის მიერ დაყენებულ დირექტორიაში გადატანის შესახებ შეტყობინებით, ფაილის კლასიფიკაცია და მისი უსაფრთხო წაშლა.

2.14 გადაწყვეტლებამ უნდა უზრუნველყოს დოკუმენტებთან მუშაობის აუდიტი File Share-ში, Cloud-სა და გარე მოწყობილობაში: უზრუნველყოს დოკუმენტების გახსნის, რედაქტირების, სახელის გადარქმევის, გადატანის, წაშლის მონიტორინგი, ღრუბლოვანი გარემოსთვის კი დამატებით უზრუნველყოს ბმულის შექმნა გაზიარებისთვის და დოკუმენტის წინასწარი გადახედვისთვის.

1. **ინტერფეისის მოთხოვნები:**

3.1. გადაწყვეტილებამ უნდა უზრუნველყოს ერთიანი ვებ ინტერფეისი სისტემისა და ინციდენტების სამართავად.

3.3. შესაძლებელი უნდა იყოს საბოლოო წერტილის აგენტების წაშლა გადაწყვეტილების ინტერფეისის გამოყენებით.

3.4. შესაძლებელი უნდა იყოს საბოლოო წერტილის აგენტების განახლება გადაწყვეტილების ინტერფეისის გამოყენებით.

1. **ინფორმაციის კლასიფიკაციის ქვესისტემის მოთხოვნები:**

4.1. გადაწყვეტილებას უნდა ჰქონდეს Microsoft Office-ის, Microsoft Outlook-ის და Web Outlook 365 ფაილების მშობლიური (“native”)კლასიფიკაცია.

4.2. კლასიფიკაცია უნდა მოხდეს ფაილის შენახვისას და არა მისი დახურვისას.

4.3. გადაწყვეტილებამ უნდა უზრუნველყოს ტექსტური დოკუმენტებისა და სურათების კლასიფიკაცია.

4.4. გადაწყვეტილებამ უნდა უზრუნველყოს Outlook-ის მოსაწვევების კლასიფიკაცია.

4.5. გადაწყვეტილებამ უნდა უზრუნველყოს მონაცემთა კლასიფიკაციისას დოკუმენტზე წყლის ნიშნის დატანის შესაძლებლობა.

4.6. გადაწყვეტილებამ უნდა უზრუნველყოს ქსელური საცავის აუდიტის შესაძლებლობა, ფაილების გახსნის, შეცვლის, წაშლისა და სახელის შეცვლის მონიტორინგი.

4.7. გადაწყვეტილებას უნდა შეეძლოს დოკუმენტების კლასიფიკაცია ბეჭდვის ოპერაციის დროს.

4.8. გადაწყვეტილებას უნდა შეეძლოს მომხმარებლის ეკრანზე წყლის ნიშნის განთავსება პოზიციის, ხილვადობის არჩევის და მთელ ეკრანზე წყლის ნიშნის განთავსების შესაძლებლობით.

4.9. გადაწყვეტილებამ უნდა შეეძლოს არა მხოლოდ ფაილების, არამედ საქაღალდეების რეალურ დროში კლასიფიკაცია.

4.10 გადაწყვეტილებამ უნდა აკონტროლოს ფაილების კოპირება ბუფერში და შეძლოს ასეთი ოპერაციის დაბლოკვა ფაილის კლასიფიკაციის დონის მიხედვით.

4.11. გადაწყვეტილებამ უნდა აკონტროლოს Microsoft Office ფაილების ეკრანის ანაბეჭდი და დაბლოკოს კლასიფიცირებული ფაილების ეკრანის ანაბეჭდის შექმნის მცდელობა.

4.12. გადაწყვეტილებას უნდა შეეძლოს თითოეული კლასიფიკაციის დონისთვის ფერის მინიჭება.

4.13. გადაწყვეტილებას უნდა შეეძლოს ფაილების ხელახალი კლასიფიკაციის აკრძალვა იმ პირებისთვის, რომლებიც კლასიფიკაციის ავტორი არ არიან.

4.14. გადაწყვეტილებას უნდა შეეძლოს კლასიფიცირებული მეილის სათაურის შეცვლა.

4.15. გადაწყვეტილებას უნდა შეეძლოს Office 365 ვებ მეილის კლასიფიკაცია.

4.16. გადაწყვეტილებას უნდა შეეძლოს მესამე მხარის (“third party”) კლასიფიკაციის სისტემებთან ინტეგრირება.

1. **დამატებითი მოთხოვნები:**

5.1. გადაწყვეტილებამ უნდა უზრუნველყოს მესამე მხარის საფოსტო სერვისებთან ინტეგრაცია სპეციალიზებული სტანდარტული პროტოკოლების (MTA) გამოყენებით.

5.2. გადაწყვეტილებამ უნდა უზრუნველყოს მესამე მხარის ვებ სერვისებთან (კარიბჭეებთან) ინტეგრაცია სპეციალიზებული სტანდარტული პროტოკოლების (ICAP) გამოყენებით.

5.3. გადაწყვეტილებამ უნდა უზრუნველყოს Office 365-ის ღრუბლოვან გარემოსთან ინტეგრაცია, ამ გარემოში კონფიდენციალურ ინფორმაციასთან დაკავშირებული ინციდენტების ნახვის შესაძლებლობით, მათ შორის OneDrive-სა და OneDrive for Business-ში ფაილებთან მუშაობის შესაძლებლობით.

5.5. გადაწყვეტილებას უნდა ჰქონდეს Off-Premice DLP ფუნქცია, ცენტრალურ კონსოლთან დაკავშირებისას, აგენტმა უნდა გამოიყენოს გარკვეული დაცვის პოლიტიკა, ხოლო off-ლაინ რეჟიმში - სხვა პოლიტიკა.

5.6. აგენტის გამოყენებით ტრაფიკის ჩაჭრა უნდა განხორციელდეს მომხმარებლის ბრაუზერში დანამატის დაყენების გარეშე.

5.7. გადაწყვეტილებას უნდა შეეძლოს თითოეული ფუნქციისთვის ფაილის სკანირების მაქსიმალური დროის ცალ-ცალკე დაყენება.

5.8. გადაწყვეტილებას უნდა შეეძლოს საკუთარი მომხმარებელთა ჯგუფების შექმნა Active Directory-თან დაკავშირების გარეშე.

5.10. გადაწყვეტილებას უნდა შეეძლოს ფაილების წაშლის შესაძლებლობის დაბლოკვა მოსახსნელი მედიიდან..

5.11. გადაწყვეტილებას უნდა შეეძლოს აგენტებისთვის ადგილობრივად დაშვებული IP მისამართების მითითების შესაძლებლობა.

5.12. გადაწყვეტილება უნდა მოიცავდეს AI ასისტენტის არსებობას.

1. **სისტემის მიწოდებისა და დანერგვის მოთხოვნები**

6.1 გადაწყვეტილება მიწოდებული უნდა იყოს „გამოწერის“ (Subscription license) ლიცენზიების სახით 1 წლის ვადით. (ფასთა ცხრილში ასევე წარდგენილი უნდა იყოს ფასი-3 წლიანი მომსახურების შემთხვევაშიც)

6.2 გაჟონვისგან დაცული ინფრასტრუქტურა მოიცავს 700-მდე მომხმარებლის სამუშაო სადგურს, რომელთაგან 300 არის Windows 2022 Terminal Servers გარემოში მომუშავე მომხმარებელი, ხოლო დანარჩენი 400 არის Windows Workstations გარემოში მომუშავე მომხმარებელი. დამატების უნდა გაკონტროლდეს 500 მომხმარებლის MS Office 365 საფოსტო ყუთი.

6.3 სისტემის დანერგვა უნდა შესრულდეს გადაწყვეტილების მიმწოდებლის სერტიფიცირებული ინჟინრის მიერ.

6.4 სისტემის დანერგვის მოთხოვნები:

* **სისტემის ზოგადი გამართვა:** მომწოდებელმა უნდა უზრუნველყოს სისტემის ყველა პროგრამული და აპარატურული კომპონენტის სრული და კორექტული ინსტალაცია და საწყისი კონფიგურაცია, დამკვეთის მიერ დამტკიცებულ არქიტექტურასთან შესაბამისობაში.
* **ფაილებისა და მონაცემთა ბაზების ფინგერპრინტინგი:** მომწოდებელი პასუხისმგებელია დამკვეთის კრიტიკული ფაილებისა და მონაცემთა ბაზების სტრუქტურებისთვის ფინგერპრინტინგის მექანიზმების დანერგვასა და კონფიგურაციაზე, რათა უზრუნველყოფილი იყოს სენსიტიური ინფორმაციის ზუსტი იდენტიფიკაცია.
* **რეგულარული გამოსახულებებისა (Regular Expressions) და ლექსიკონების დანერგვა:** მომწოდებელმა უნდა შეიმუშაოს, დანერგოს და დააკონფიგურიროს რეგულარული გამოსახულებებისა (Regular Expressions) და სპეციალიზებული ლექსიკონების ნაკრები, რომლებიც საჭიროა კონფიდენციალური მონაცემების ეფექტური აღმოჩენისა და კლასიფიკაციისათვის, დამკვეთის მოთხოვნებთან შესაბამისობით.
* **კლასიფიკაციის სტრატეგიის დანერგვა:** მომწოდებელმა უნდა დანერგოს დამტკიცებული მონაცემთა კლასიფიკაციის სტრატეგია, ინტეგრირება მოახდინოს დამკვეთის არსებულ საინფორმაციო სისტემებთან და უზრუნველყოს სენსიტივობის ნიშნების (labels) ავტომატური ან ნახევრად ავტომატური მინიჭება.
* **პოლიტიკების ოპტიმიზაცია:** დანერგვის ეტაპზე მომწოდებელმა უნდა განახორციელოს შემუშავებული უსაფრთხოების პოლიტიკების ოპტიმიზაცია, რათა მინიმუმამდე დაიყვანოს მცდარი დადებითი აღმოჩენები (false positives) და მაქსიმალურად გაიზარდოს დეტექციის ეფექტიანობა, დამკვეთის წარმომადგენლებთან მჭიდრო თანამშრომლობით.
* **კორპორატიული ელფოსტის ინსპექციის დანერგვა:** მომწოდებელმა უნდა ინტეგრიროს და დააკონფიგურიროს კორპორატიული ელფოსტის შიგთავსის ინსპექტირების ფუნქციონალი, რათა უზრუნველყოფილი იყოს ამ არხით სენსიტიური ინფორმაციის გადაცემის მონიტორინგი და კონტროლი.
* **მონაცემების აღმოჩენის (Data Discovery) დანერგვა:** მომწოდებელმა უნდა უზრუნველყოს Data Discovery ფუნქციონალის სრული დანერგვა, დამკვეთის მონაცემთა საცავების სისტემატური სკანირებისა და ინდექსაციისთვის, რათა გამოვლინდეს და კატალოგიზდეს ყველა სენსიტიური ინფორმაცია როგორც სტრუქტურირებულ, ისე არასტრუქტურირებულ წყაროებში.

6.5 გადაწყვეტილების მიმწოდებელმა ასევე უნდა წარმოადგინოს მწარმოებლის ავტორიზაციის წერილი (Manufacturer Authorization Form), რომელიც დაადასტურებს მის უფლებებს გადაწყვეტილების მიწოდებაზე.