Cartubank-ის ტექნიკური დავალება მონაცემთა გაჟონვის პრევენციის (DLP) სისტემის შესყიდვისათვის

1. მიზანი

წინამდებარე ტექნიკური დავალების მიზანია ორგანიზაციის ინფორმაციული აქტივების დაცვის უზრუნველსაყოფად მონაცემთა გაჟონვის პრევენციის (DLP) სისტემის შესყიდვა, დანერგვა და მხარდაჭერა. სისტემა უნდა უზრუნველყოფდეს კონფიდენციალური ინფორმაციის იდენტიფიცირებას, მონიტორინგს, კონტროლს და მონაცემთა გაჟონვის პრევენციას როგორც შიდა, ისე გარე არხებით.

---

2. სამუშაოს მოცულობა

პროექტის ფარგლებში მომწოდებელმა უნდა უზრუნველყოს:

- DLP სისტემის ლიცენზიების მიწოდება (650 მომხმარებელზე);
- სისტემის ინსტალაცია და კონფიგურაცია;
- არსებული ინფრასტრუქტურასთან ინტეგრაცია;
- ტექნიკური პერსონალის გადამზადება;
- გარანტირებული ტექნიკური მხარდაჭერა.

---

3. სისტემის ძირითადი ფუნქციონალი

3.1 მონაცემთა იდენტიფიკაცია და კლასიფიკაცია

- კონფიდენციალური მონაცემების იდენტიფიკაცია (PII, ფინანსური, საბანკო, კომერციული საიდუმლო, რეგულაციებით განსაზღვრული მონაცემები).
- მონაცემთა კლასიფიკაციის მხარდაჭერა (სპეციალურად განსაზღვრული სახელების მინიჭება, ავტომატური კლასიფიკაცია შაბლონების საფუძველზე).
- რეგულაციებთან შესაბამისობა (GDPR, PCI DSS, ISO 27001 და სხვა).

3.2 პოლიტიკების მართვა

- ცენტრალიზებული პოლიტიკების შექმნა და ადმინისტრირება.

- პოლიტიკების დიფერენცირება მომხმარებლის, ჯგუფის, განყოფილების ან სისტემის მიხედვით.
- კონტროლის მექანიზმები:
    - **Block** – მონაცემის გადაგზავნის/გატანის აკრძალვა;
    - **Quarantine** – მონაცემის იზოლირება;
    - **Alert/Notify** – გაფრთხილება ადმინისტრატორისთვის და/ან მომხმარებლისთვის;
    - **Audit** – მხოლოდ მონიტორინგი.

3.3 არხების მონიტორინგი და კონტროლი

სისტემა უნდა უზრუნველყოფდეს მონაცემთა მოძრაობის კონტროლს შემდეგ არხებზე:

- ელ.ფოსტა (SMTP, Exchange, O365, Gmail და სხვა);
- ქსელური ტრაფიკი (HTTP/HTTPS, FTP, IM, cloud services);
- ფიზიკური მედია (USB, CD/DVD, გარე დისკები);
- პრინტერი და Print Screen ფუნქცია;
- Endpoint აპლიკაციები (MS Office, PDF, ZIP, social media clients და სხვა).

3.4 Endpoint დაცვა

- Windows, Linux და macOS Endpoint-ების მხარდაჭერა;
- პოლიტიკების ავტომატური გამოყენება ლეპტოპებზე, მათ შორის ქსელიდან გარეთ ყოფნისას;
- მონაცემების დაშიფვრის მხარდაჭერა USB/გარე მოწყობილობებზე.

3.5 რეპორტინგი და აუდიტი

- დეტალური ლოგირების სისტემა;
- Dashboards რეალურ დროში;
- ავტომატური ანგარიშგება (PDF/Excel ფორმატში);
- ინციდენტების ძიება და ანალიტიკა.

---

4. ინტეგრაცია

DLP სისტემა უნდა ინტეგრირდეს ორგანიზაციის შემდეგ ინფრასტრუქტურასთან:

- Active Directory (LDAP/AD);
- SIEM სისტემები (მაგ: Splunk, QRadar, Elastic);
- ელ.ფოსტის სერვერები (Exchange, O365, Google Workspace);
- Proxy/Firewall გადაწყვეტები.

---

5. ადმინისტრირება და გამოყენება

- ერთიანი ადმინისტრირების კონსოლი (Web-based);
- RBAC (Role-Based Access Control);
- ინციდენტების workflow და ესკალაციის მექანიზმი;
- მრავალენოვანი ინტერფეისი (სავალდებულო – ინგლისური, სასურველი – ქართული).

---

6. სხვა მოთხოვნები

- მაღალი ხელმისაწვდომობა (HA) და Load Balancing მხარდაჭერა;
- განახლებების ავტომატური მიღება და ინსტალაცია;
- მაქსიმალური დატვირთვა თითოეულ კომპიუტერზე არაუმეტეს 15%.

---

7. უსაფრთხოების მოთხოვნები

- მონაცემთა დაშიფვრა (AES-256 ან უფრო მაღალი);
- კომუნიკაციის უსაფრთხოება TLS 1.2/1.3 პროტოკოლებით;
- ადმინისტრატორის ქმედებების აუდიტი;
- Failover/DR მხარდაჭერა.

---

8. ტრენინგი და მხარდაჭერა

- მინიმუმ 2-დღიანი ტრენინგი სისტემის ადმინისტრატორებისა და უსაფრთხოების გუნდისთვის;
- სისტემის დოკუმენტაცია ქართულ და/ან ინგლისურ ენაზე;
- ტექნიკური მხარდაჭერა 24/7 რეჟიმში მინიმუმ 1 წლის განმავლობაში.

---

9. მიწოდების ვადები

- სისტემის მიწოდება და ინსტალაცია – ხელშეკრულებიდან არაუგვიანეს 45 კალენდარული დღისა.
- სატესტო რეჟიმი – მინიმუმ 7 დღე.
- საბოლოო ჩაბარება – ტესტირების წარმატებით დასრულების შემდეგ.

---

10. შეფასების კრიტერიუმები

ტენდერში გამარჯვებული კომპანია განისაზღვრება შემდეგი კრიტერიუმების მიხედვით:

- ტექნიკური შესაბამისობა მოცემულ მოთხოვნებთან;
- კომპანიის გამოცდილება მსგავს პროექტებში;
- შემოთავაზებული ფასის კონკურენტუნარიანობა;
- მხარდაჭერის პირობები.