חירייה פארק המחזור
איגוד ערים דן לתברואה
נוסד בשנת 1966

מכרז פומבי מס' 1/2026

רכש מערכת הגנה, בקרה, זיהוי ותגובה לאירועי סייבר כולל שירות MDR מנוהל

הבהרה מס' 3

על פי סמכותו באמור בתנאי המכרז שבנדון, מתכבד בזאת איגוד ערים אזור דן (תברואה וסילוק אשפה) (להלן: "המזמין" ו/או "האיגוד"), למסור למשתתפי המכרז מענה לשאלות הבהרה שהתקבלו.

מובהר ומודגש בזאת כי מסמך זה מהווה תוספת למסמכי המכרז ומהווה חלק בלתי נפרד מהמכרז וכי בכל מקרה של סתירה, גובר האמור בהודעה זו על האמור במסמכי המכרז ו/או על האמור בהודעה מוקדמת יותר.

א. מענה לשאלות הבהרה:

מס'	מס' עמ'	סעיף במכרז/ הסכם	פירוט השאלה	תשובה
.1	3 31	2.7	ביחס לתשובה מס' 105 למסמך ההבהרות, ולצורך תמחור רכיב SIEM CLM, נבקש להבהיר כי מאחר שלא נמסרו נתוני EPS או Gigabytes Per Day מחייבים, האם המציע רשאי להגדיר בהצעתו תקרת נפח לוגים כלולה, תקרת EPS או Gigabytes Per Day, תקופת שמירה ומקורות לוגים כלולים?	הבקשה מתקבלת.
.2	3 31	2.7	בהמשך לשאלה הנזכרת לעיל, האם רשאי המציע לתמחר למשל עד 500 EPS, וכן שמירת לוגים משך 6 חודשים בתצורת "חם" ו-12 חודשים בתצורת "קר"?	90 יום חם 365 יום ארכיון (קר)
.3	3 31	2.7	בנוסף נבקש לאשר כי כל חריגה מהתקרה שהוגדרה על ידי המציע, לרבות גידול בנפח הלוגים, הארכת תקופת השמירה, חיבור מקורות לוג נוספים או דרישה לשמירת כלל הנתונים מכל המקורות, תתומחר בנפרד בהתאם למודל התמחורי שיוצג בהצעת המציע	הבקשה מתקבלת
.4	3 31	2.7	תקופת שמירת מקורות לוגים – לצורך תמחור רכיב SIEM CLM ואחסון הלוגים נבקש להבהיר מהי תקופת שמירת הלוגים המינימלית הנדרשת לאחור?	90 יום חם 365 יום ארכיון

חירייה פארק המחזור
איגוד ערים דן לתברואה
נוסד בשנת 1966

מס'	מס' עמ'	סעיף במכרז/ הסכם	פירוט השאלה	תשובה
			נבקש לפרט האם נדרשת שמירה ל- 30 יום, 90 יום, 180 יום, 12 חודשים או תקופה אחרת הן לצורך אספקת השירות הנדרש והן לצורך תמחור ההצעה	
.5	3 31	2.7	בנוסף נבקש להבהיר האם כלל הלוגים נדרשים להיות זמינים לחיפוש מיידי לאורך כל תקופת השמירה או שניתן לשלב בין שמירה חמה לחיפוש מיידי לבין שמירה בארכיון	90 יום חם 365 יום ארכיון
.6	3 31	2.7	ככל שלא מוגדרת תקופת שמירה מחייבת נבקש לאשר כי המציע רשאי להגדיר בהצעתו את תקופת שמירת הלוגים הכלולה במחיר וכל הארכה מעבר לכך תתומחר בנפרד בהתאם למודל התמחור שיוצג בהצעה	90 יום חם 365 יום ארכיון

<u>הערה כללית לנושא מערכתSIEM / CLM</u>

האיגוד מבקש יכולת תחקור, ניתוח וזיהוי אירועי סייבר, ולשם כך מוגדרת הדרישה למערכת SIEM נדרש מנגנון איסוף, ריכוז וחיפוש לוגים <u>הרלוונטיים לאירועי אבטחת מידע</u>, כולל יכולות קורלציה ותחקור אירועים.

נדרש Retention של לפחות 90 יום לחיפוש מיידי (Hot) ועד 12 חודשים ארכיון(Cold)

בכבוד רב,

אלון לוי, סמנכ"ל תפעול

על המציעים לצרף הבהרה זו בשהיא חתומה על ידו במסגרת הגשת הצעתם למכרז.

חתימה + חותמת _____ תאריך _____