מרכז החישובים הבינאוניברסיטאי

מכרז פומבי מס' 2-2023

שירותי IR\IRT למחב"א והמוסדות האקדמאים החברים בה

תוכן העניינים

תקציר מנהלים (I) 5
1. מנהלה 5
1.1 כללי 5
1.1.1 שלבי המכרז 6
1.1.2 טבלת ריכוז מועדי המכרז 6
1.2 הגדרות, קיצורים ומונחים טכניים 6
1.2.1 הגדרות 6
1.2.2 קיצורים ומונחים טכניים 7
1.3 ניהול המכרז 8
1.3.1 קבלת מסמכי המכרז 8
1.3.2 עורך המכרז 8
1.3.3 נוהל העברת שאלות ובירורים 8
1.3.4 מסירת ההצעות (M) 9
1.4 ניהול המכרז 9
1.5 אופן המענה 10
1.6 תנאי סף להשתתפות במכרז ואישורים שעל המציע להמציא עם הגשת ההצעה 11
1.6.1 כללי 11
1.6.2 מעמדו המשפטי של המציע 11
1.6.3 עמידה בהוראות חוק עסקאות גופים ציבוריים ושמירה על דיני עבודה 12
1.6.4 דרישות סף מקצועיות מהמציע (M) 12
1.6.5 תצהיר בדבר היעדר ניגוד עניינים 14
1.6.6 תצהיר כללי 15
1.6.7 תצהיר בדבר העסקת אנשים עם מוגבלות 15

1.6.8 תצהיר בדבר זמינות מיידית ... 15
1.6.9 תצהיר בדבר העדר תביעות והליכי פשיטת רגל (M) ... 15
1.6.10 אישור רו"ח על היעדר הערת עסק חי בדוחות הכספיים של המציע (M) ... 15
1.6.11 ריכוז אישורים ומסמכים שנדרש לצרף להצעה (M) ... 15
1.7 בדיקת ההצעות והערכתן ... 16
1.8 תוקף ההצעה ... 17
1.9 הסכם התקשרות חתום בראשי תיבות ... 17
1.9.1 מועד כניסת ההתקשרות לתוקף ... 17
1.10 זכויות עורך המכרז (I) ... 18
1.10.1 ביטול המכרז ... 18
1.10.2 שאלות הבהרה ... 18
1.10.3 פסילת הצעה ... 18
1.10.4 היקף ההתקשרות ... 18
1.11 הצעת הספק ... 19
1.11.1 מבנה כללי ... 19
1.11.2 מספר עותקים ... 19
1.12 בעלות על המכרז ועל ההצעה (I) ... 19
1.12.1 בעלות על מסמכי המכרז והשימוש בהם ... 19
1.12.2 בעלות על ההצעה ושימוש בה ... 20
1.12.3 חשיפת פרטי הצעה לצדדים שלישיים ... 20
1.13 מחירים ... 20
1.14 תקופת ההתקשרות ... 20
1.15 היררכיה בין מסמכים, פרשנות וסמכות שיפוט ... 20
.2 יעדים, מטרות והליכים (I) ... 21
2.1 כללי ... 21
.3 SOW – תיחום ... 21
3.1 מכלול השירותים (M) ... 21
3.1.1 תכולת השירותים הנדרשת - מכלול חובה ... 21
3.1.2 תהליך חקירה, טיפול והכלת אירוע – תיאור כללי ... 23
3.1.3 תהליך חקירה, טיפול והכלת אירוע – תהליך מפורט (S) ... 24
3.1.4 תהליך התנעה מול מוסד אקדמאי (S) ... 24
3.1.5 פריסת כלים ומנגנונים שונים (S) ... 25

3.1.6 הדרכות והעשרות (S) 25
3.1.7 השתתפות בסימולציות (M) 25
3.1.8 בנייה ותחזוקת "תיק אתר" IR - תכולות, נכסים, מידע רלוונטי (M) 25
3.1.9 שיתוף פעולה עם צוותי IR/מו"מ אחרים (M) 26
3.1.10 דוחות וישיבות היגוי (M) 26
3.1.11 סודיות, תקשורת ודוברות (M) 26
3.1.12 אישור ביטוח סייבר (S) 27
.4 נסיון במגזר האקדמי (בהתייחס למודל "החופש האקדמאי") (S) 27
.5 מתודולוגיה וחקירת אירועים (S) 27
.6 צוות IRT – דרישות ומשימות 27
6.1 צוות IRT (M) 27
6.2 עדכון על שינוי ציוות/מצבת כ"א (M) 28
.7 IR Playbook & DFIR (S) 29
7.1 יצירה/השבחה של נהלי IR ופרוטוקולי תגובה/בלימה 29
7.2 בניית IR Playbook (M) 29
7.3 תיאור ותיוג אירועים ואיומים בפועל (S) 29
7.4 פרוטוקולים להכלה ובלימת אירוע (S) 29
7.5 קובץ תרחישים ואסקלציה מבוסס MS Visio (S) 29
7.6 מטריצת איומים מינימלית (S) : 30
7.7 תיעוד אירוע ותהליכים (M): 30
7.8 הפעלת נוהל DFIR לשמירת רצף עדויות ושימור מידע פורנזי (S) : 31
7.9 איסוף וגיבוי עדויות פורנזיות (M) : 33
.8 מוסדות אקדמאיים ופריסה גיאוגרפית 36
8.1 רשימת המוסדות האקדמאיים הרלוונטיים (I) 36
8.2 פיזור גיאוגרפי של קמפוסים (I) 37
.9 תכולת שירותים אופציונליים (G) 38
.10 היפרדות 38
.11 עלות 39
11.0 כללי 39
11.0.1 אופן התשלום 39
נספח 1.3.3 גלופה להעברת שאלות ובקשות הבהרה 40
נספח 1.6.2 מעמדו המשפטי של המציע 41

נספח 1.6.3 - עמידה בהוראות חוק עסקאות גופים ציבוריים ושמירה על דיני עבודה 42
נספח 1.6.4 – תצהיר בדבר ניסיון המציע.. 44
נספח 1.6.5 תצהיר בדבר היעדר ניגוד עניינים.. 45
נספח 1.6.6 תצהיר כללי 47
נספח 1.6.7 - תצהיר בדבר העסקת אנשים עם מוגבלות.. 49
נספח 1.6.8 תצהיר בדבר זמינות מיידית.. 50
נספח 1.6.9 תצהיר בדבר העדר תביעות והליכי פשיטת רגל.. 51
נספח 1.7 מפל – ניקוד איכות... 52
נספח 1.9 הסכם התקשרות... 53
נספח 11 - מענה כספי 54
נספח 12 – תמחור שירותים אופציונאליים... 55

תקציר מנהלים (I)

מחב״א – מרכז החישובים הבינאוניברסיטאי [להלן : ״**מחב״א**״ או ״**המזמינה**״] , יוצאת בזאת במכרז פומבי לשירות IRT – Incident Response Team לבחירת ספק IR/IRT עבור תשעת המוסדות החברים בה [להלן : ״**המוסדות**״], הכל כמפורט במסמכי המכרז זה ובנספחיו ובהסכם המצורף אליו.

למוסדות החברים במחב״א שמורה הזכות, לפי שיקול דעתם שלא להתקשר עם הזוכה במכרז זה.

המכרז הינו לאספקת שירותי IR/IRT כוללים ומענה לאירועי סייבר בסביבה האקדמאית.

כחלק מפעילות היערכות לאירועי סייבר, פועלת מחב״א ליצירת תשתית מסחרית וטכנית להתקשרות עם חברות בעלות מומחיות בתחום ה IR/IRT שישמשו לתמיכה בגופי אבטחת המידע במוסדות במקרה של אירוע סייבר. השירות שיירכש ישמש לסיוע באפיון וזיהוי איום, רישום וניהול האירוע, איסוף פורנזיקה וממצאים, בלימה, הכלה והתאוששות.

השירות יפעל בהלימה ובסנכרון מלא לגופי אבטחת המידע הפנימיים במוסדות הרלוונטיים ובקמפוסים השונים, בהתאמה למדיניות הסייבר והביטחון באותם גופים ולסביבות הייחודיות הכוללות את ״החופש האקדמאי״ והאוטונומיה המתאפשרת בסביבות אלו.

אופי השירות יכלול הגעה פיזית לאתר תחת הגדרת SLA ובהתאם לנסיבות.

מחב״א שומרת לעצמה את הזכות לבטל את המכרז בכפוף לתהליך פנימי בכל שלב.

רשאי להגיש הצעה מציע אשר הינו יצרן או ספק (או שילוב של יצרנים-ספקי /שירות) העומדים בדרישות הקדם המפורטות במכרז.

הספק הזוכה יחתום על הסכם עם מחב״א שבאמצעותו יעניק שירות למחב״א, למוסדות וללקוחות מחב״א.

1. מנהלה

1.1 כללי

מחב״א מזמינה בזאת הצעות לשירות IRT – Incident Response Team לבחירת ספק IR/IRT מוביל כמפורט במסמכי מכרז זה (להלן : ״**המכרז**״).

מחב״א מאוגדת כעמותה וחברות בה תשע האוניברסיטאות שלהלן : טכניון, אוניברסיטת חיפה, אוניברסיטה הפתוחה, אוניברסיטה העברית, אוניברסיטת בר-אילן, מכון ויצמן למדע, אוניברסיטת תל-אביב, אוניברסיטת בן גוריון ואוניברסיטת אריאל (להלן : ״**המוסדות**״).

התקשרות מחב״א עם הזוכה במכרז תעשה עבורה ועבור המוסדות. המוסדות החברים רשאים אך אינם מחויבים לאמץ את תוצאות המכרז.

בכל מקום במסמך זה או בהסכם הנלווה בו מופיעה המילה ״מחב״א״, האמור יהיה נכון גם למוסדות וללקוחות מחב״א שיצטרפו לשירות[להלן ״**הלקוחות**״]. כל התחייבויות המציע יראו אותן כהתחייבויות עבור מחב״א, המוסדות וללקוחות יחד ולחוד וכל זכות שנתונה למחב״א על פי ההסכם תהיה נתונה גם למוסדות וללקוחות שיצטרפו לשירות.

מובהר בזאת כי הסכם ההתקשרות עם הספק/ים הזוכ/ים יחתם עם מחב״א בלבד, בעוד השירות יסופק למחב״א, למוסדות וללקוחות.

מחב״א ו/או המוסדות אינם מתחייבים להיקף הזמנות כלשהן ואין בזכייה במכרז ו/או בחתימה על ההסכם כדי להבטיח מתן שירותים ע״י הספק בהיקף כלשהו או בכלל.

המכרז ינוהל על ידי ועדת המכרזים של מחב״א [להלן : ״**ועדת המכרזים**״] על פי נוהל המכרזים של מחב״א [להלן ״**הנוהל**״ או ״**נוהל המכרזים**״] שאותו ניתן למצוא באתר מכרזים של מחב״א.

מאחר וזהו מכרז בעל מורכבות טכנולוגית מיוחדת וכזה הדורש יחסי אמון מיוחדים החליטה ועדת המכרזים, לאור הוראות הסעיפים 12.1.1 ו-12.1.6, לנוהל המכרזים כי היא תהיה רשאית לנהל מו״מ עם המציעים שהצעותיהם תיראנה לה מתאימות .

מכרז זה הנו מכרז דו שלבי. לפיכך רק לאחר שוועדת המכרזים תסיים את קביעת ציוני האיכות של הצעות המציעים תפתח ועדת המכרזים את ההצעות הכספיות.

1.1.1 שלבי המכרז

א. פרסום המכרז

ב. הליך הבהרות – כמפורט להלן בסעיף 1.3.3.

ג. הגשת הצעות – מציעים אשר עומדים בתנאי הסף של מכרז זה, יגישו את הצעותיהם בהתאם לדרישות המפורטות במסמכי המכרז.

ד. בחינת עמידה בתנאי סף - מציעים שוועדת המכרזים תמצא כי לא עמדו באחד או יותר מתנאי הסף – יפסלו, והצעותיהן לא תשתתפנה בהמשך הליך בחירת הספק הזוכה.

ה. בחינה מפורטת ושקלול - מציעים שוועדת המכרזים תמצא כי עמדו בכל תנאי הסף יעברו הליך בחינה מפורט ושקלול איכותי וכלכלי משולב, שבסופו ייבחר הספק הזוכה במכרז.

1.1.2 טבלת ריכוז מועדי המכרז

פעילות	תאריך
מועד פרסום המכרז	23/07/2023
מועד אחרון להעברת שאלות ובירורים בהקשר למסמכי המכרז	13/08/2023
מועד אחרון להעברת תשובות מחב״א לשאלות ובירורים של מציעים	27/08/2023
מועד אחרון להגשת הצעות לתיבת המכרזים	14/09/2023 בשעה 13:00
מועד תוקף ההצעה	30/04/2024

במקרה של אי התאמה בין הרשום בטבלה לעיל לבין הרשום בגוף המכרז, יקבעו הנתונים הרשומים בטבלה לעיל. ועדת המכרזים תהיה רשאית, על סמך שיקול דעתה המוחלט, לשנות כל אחד מהמועדים המפורטים בטבלה לעיל, ובכלל זה לדחות את המועד האחרון להגשת ההצעות למכרז. הודעה בדבר שינויים כאמור תפורסם באתר המכרזים של מחב״א.

1.2 הגדרות, קיצורים ומונחים טכניים

הגדרות, קיצורים ומונחים טכניים אלה יחולו על המכרז ונספחיו (למען הסר ספק מובהר בזאת כי, בכל הנוגע לתכולת העבודה המפורטת, יחולו בנוסף ההוראות הכלולות במפרט ובנספחיו).

1.2.1 הגדרות

מונח	פירוט
איש קשר	הגורם מטעם המציע אשר מונה לנהל את המכרז מול מחב״א.
הצעה	תשובת המציע להזמנה להציע הצעות על כל נספחיה.
מחב"א ו/או הלקוח ו/או המזמינה	מרכז החישובים הבינאוניברסיטאי.
מוסדות	אחד או יותר מהמוסדות האקדמיים החברים במחב״א: הטכניון, אוניברסיטת חיפה, אוניברסיטה הפתוחה, אוניברסיטה העברית, אוניברסיטת בר-אילן, מכון ויצמן למדע, אוניברסיטת תל-אביב, אוניברסיטת בן גוריון ואוניברסיטת אריאל.
לקוחות	כל מוסד אקדמי אשר יזמין מהזוכה/זוכים במכרז טובין ו/או שירותים באמצעות התקשרות שבין מחב״א לספק הזוכה בין אם הוא מוסד חבר ובין אם לא.
[ה]מכרז ו/או (ה)מפרט או הבלי"מ	מסמך זה על נספחיו דרישותיו תנאיו, חלקיו ונספחיו.
מפ״ל - מפרט פנימי לבדיקה	מגדיר את אופן בדיקת האיכות של הצעות המציעים במכרז שעמדו בתנאי הסף המנהלתיים.
מציע	מגיש/ים הצעה במכרז.
ספק ו/או החברה	המציע/ים שזכה במכרז.

עורך המכרז	האחראי למכרז זה מטעם "מחב"א"
IR	טיפול ומענה לאירועי סייבר Incident Response
IRT	צוות תגובה וניהול אירוע באתר לקוח, – Incident Response Team צוות מורכב מראש צוות, סגן ואנשי חקירות סייבר
Time Zone	איזור זמן המגדיר זמן תגובה והגעה לאתר (SLA)
תקופת התקשרות	פרק הזמן מיום חתימת ההסכם עם הספק ועד היום האחרון לתוקף ההתקשרות

1.2.2 קיצורים ומונחים טכניים

תיאור	ראשי תיבות
Artificial Intelligence	AI
Application Layer Gateway	ALG
Application Programming Interface	API
Application Grade DDOS Protection	APP-DDOS-P
Advanced Persistent Threat	APT
Command & Control	C&C
Content Disarm & Reconstruct	CDR
Continues Integration/Continuous Development (Devops Terms)	CI/CD
Cyber Intelligence/Threat Intelligence	CI/TI
Critical Infrastructure Protection	CIP
Domain Name Generation Attack	DGA
Defense In Depth	DID
Domain Name System	DNS
Denial of Service/Distributed Denial of Service	DOS/DDOS
Endpoint Detection & Response	EDR
Extended Detection & Response	XDR
End Point Protection (EPS/NG AV)	EPP
Full Packet Capture (Big Data)	FPC
Chain of Custody (Forensics)	COC
Industrial Control Systems	ICS
Indication Of Compromise	IOC
Incident Response/ Incident Response Team	IR/IRT
Information Technology/Information Communication Technology	IT/ICT
Metadata	MD
Mean Time to Identify/Contain	MTTI/MTTC
Network Behaviour Analysis	NBA
Network Behaviour Anomaly Detection	NBAD
Network Detection & Response	NDR
Network Grade DDOS Protection	NET-DDOS-P
Next Generation Network Based Intrusion Prevention System	NG NIPS
Next Generation Firewall	NGFW
Network Operation Center	NOC
Operational Technologies	OT
Personally Identifiable Information	PII
Digital Forensics Incident Response	DFIR

מסמך זה הוא רכושה הבלעדי של מחב"א

SIEM	Security Information & Event Management
SOAR	Security Orchestration, Automation & Response
SOC	Security Operation Center
SWG	Secure Web Gateway
TTPs	Tactics/Tools, Techniques and Procedures
UBA	User Behaviour Analysis
VPC	Virtual Private Cloud
VM/RM	Vulnerability Management / Risk Management
WAF	Web Application Firewall
T1	נקודת זמן ראשונית לפתיחת אירוע
CA1	אזור/כיסוי גאוגרפי מרכז (חדרה – גדרה כולל ירושלים)
NA1	אזור/כיסוי גאוגרפי צפון (חדרה – חיפה)
SA1	אזור/כיסוי גאוגרפי דרום (גדרה – באר שבע)
EX1	אזור/כיסוי גאוגרפי צפונית לחיפה ודרומית לב״ש (למעט אילת)
EX2	אזור/כיסוי גאוגרפי אילת

1.3 ניהול המכרז

1.3.1 קבלת מסמכי המכרז

את מסמכי המכרז ניתן לקבל באופן אלקטרוני באמצעות פנייה למשרד מחב״א

טלפון: 03-6460555 או ל- e-Mail: IUCC-Secretariat@mail.iucc.ac.il

או להוריד מאתר האינטרנט של מחב״א בכתובת : http://www.iucc.ac.il/he/tender

1.3.2 עורך המכרז

נציגת מחב״א למכרז זה היא: רו״ח אפרת פיינשניידר

טלפון: 03-6460558, דוא״ל: efratf@mail.iucc.ac.il

1.3.3 נוהל העברת שאלות ובירורים

א. שאלות הבהרה ניתן להעביר בדוא״ל בלבד עד ולא יאוחר מהתאריך הנקוב בטבלה 1.1.2.

ב. שאלות מציעים תוגשנה בכתב ע״ג נספח שאלות הבהרה המצורף כקובץ אקסל למסמכי המכרז, ותועברנה באמצעות דואר אלקטרוני לעורך המכרז, בכתובת tender@iucc.ac.il. המציע יציין את הסעיף המדויק אליו מתייחסת כל שאלה באופן הבא:

מס׳ שאלה	סוג המסמך	הסעיף במסמך	ס״ק	השאלה
1.	מפרט	2.3.6.1	ג׳	דוגמא <<<
2.	הסכם	14	ב׳	דוגמא <<<
3.	נספח...	1.2	ד׳ 1.	דוגמא <<<

ג. תשובות ועדת המכרזים לשאלות הבהרה (ככל שמחב״א תמצא לנכון להשיב להן), יפורסמו באתר המכרזים של מחב״א בכתובת: http://www.iucc.ac.il/he/tender, [להלן: ״**האתר**״] מבלי לחשוף את זהות הפונה.

ד. תשובות ועדת המכרזים יחשבו חלק ממסמכי המכרז. באחריות המציע לוודא כי שאלתו הגיעה ליעדה ולקבל אישור על כך. באחריות מציעים להתעדכן בתשובות לשאלות הבהרה שיפורסמו באתר.

ה. ועדת המכרזים לא תשיב לפניות שיומצאו לה לאחר המועד האחרון להעברת שאלות ובירורים.

ו. ועדת המכרזים תשיב לפניות מהר ככל הניתן ועד למועד המצוין בטבלת ריכוז מועדי המכרז שבסעיף 1.1.2, בשורה "מועד אחרון להעברת תשובות מחב"א לשאלות ובירורים של מציעים"

ז. רק תשובות של ועדת המכרזים שתפורסמנה ע"י עורך המכרז באתר מחב"א מחייבות את מחב"א והן תהווינה חלק בלתי נפרד ממסמכי המכרז.

ח. לאור שאלות ההבהרה שיתקבלו, תשקול ועדת המכרזים לקיים כנס מציעים ובאם תחליט לעשות כן - ומובהר בזאת כי לא תהיה חייבת לעשות זאת - תפרסם את החלטתה באתר מחב"א לא יאוחר מאשר 6 ימי עבודה לאחר המועד האחרון להגשת שאלות ההבהרה [מועד המצוין בטבלת ריכוז מועדי המכרז שבסעיף 1.1.2].

ט. ועדת המכרזים תהיה רשאית, על פי שיקול דעתה המוחלט והבלעדי, להחליט, לאחר פרסום המכרז, על תיקונים, הבהרות, שינויים ותוספות בתנאי המכרז, ומעת שתפרסם החלטתה באתר יהוו אלו חלק בלתי נפרד ממסמכי המכרז. המציע יצרף למסמכי הצעתו את הודעות ועדת המכרזים וכל מסמך שהוסף כאמור, כשהם חתומים בחתימתו, לאישור קבלתם, הבנתם, והבאת האמור בהם בחשבון במסגרת הצעתו. שינויים, הבהרות ועדכונים כאמור לעיל, יפורסמו באתר ועל המבקשים להשתתף במכרז, לעקוב אחר העדכונים באתר כאמור לעיל. חובת המציע, לוודא באתר, בטרם הגשת ההצעה, האם נערכו שינויים כל שהם למכרז, לפני ולקראת המועד האחרון להגשת ההצעות ולא תהיה למציע כל טענה או תביעה כלפי מחב"א בגין אי משלוח הודעות לדואר אלקטרוני, בקשר למכרז.

1.3.4 מסירת ההצעות (M)

א. על המציע להכניס, בעצמו או באמצעות שליח, את הצעתו – שתערך ותיארז באופן האמור בסעיף 1.11.2 שלהלן - לתיבה המיועדת לכך, במשרדי מחב"א, בניין הנדסת תוכנה, אוניברסיטת תל אביב (קומה 4), עד ולא יאוחר מהיום והשעה הנקובים בטבלה 1.1.2. אין למסור הצעות בכל דרך אחרת. הצעה שלא תוכנס לתיבת המכרזים עד למועד האמור תפסל על הסף. על המציע להביא בחשבון עיכוב אפשרי בשל הבידוק הביטחוני בקמפוס.

ב. מציע המבקש להגיש הצעתו, נדרש להגישה על גבי מסמכים התואמים לפסקאות ודרישות המכרז לפי הסיווג כפי שנמסר על ידי מחב"א, לחתום בתחתית כל עמוד בכל אחד ממסמכי המכרז, להכניסם יחד עם יתר המסמכים הדרושים כאמור במכרז זה למעטפה סגורה וחתומה, ללא זיהוי חיצוני, ולסגור את מעטפת ההצעה. אין לכתוב או לסמן דבר על גבי מעטפת ההצעה מלבד מספר המכרז ונושא המכרז.

ג. הצעת המציע תהיה בתוקף עד למועד המופיע בטבלה 1.1.2 בשורה "מועד תוקף ההצעה". מובהר כי גם לאחר שמחב"א תתקשר בהסכם עם מציע כלשהו (אם תתקשר), ותודיע למי מהמציעים כי הצעתו נדחתה, לא יפקעו הצעות שהוגשו על פי מכרז זה ולא זכו, במשך התקופה האמורה. **ועדת המכרזים תהא רשאית (אך לא חייבת) לבחור יותר מזוכה אחד**. בנוסף, תהיה ועדת המכרזים זכאית לבחור זוכים נוספים, למקרה שהסכם ההתקשרות עם הזוכה הראשון או השני וכן הלאה לא ייצא לפועל, מכל סיבה שהיא, או יבוטל ע"י מחב"א בתוך 12 חודשים מיום תחילתו. בחלוף המועד האמור, תהיה ועדת המכרזים רשאית לבחור בהצעה הבאה בטיבה כאמור לעיל ובלבד שהמציע של הצעה זו נתן לכך את הסכמתו לפנייה של מחב"א בכתב.

ד. הגשת הצעה חתומה תהווה ראיה חלוטה לכך שהמציע קרא והבין את כלל מסמכי המכרז ובחר לתת להם את הסכמתו, באופן מלא ושלם וללא הסתייגויות כלשהן.

ה. הצעת המחיר תוגש באמצעות מילוי נספח 11 וחתימה עליו .

1.4 ניהול המכרז

א. זכות העיון בהצע/ות הזוכ/ות נתונה למציע המשתתף במכרז, וזאת בתנאים ובמגבלות המפורטים בנוהל המכרזים של מחב"א. לבקשה לעיון כאמור תצורף המחאה לפקודת מחב"א בסך 500 ש"ח לכיסוי העלות הכרוכה בכך.

ב. מציע הסבור כי אין לאפשר עיון בחלקים של הצעתו שכן עיון בהם עלול לחשוף סודות מסחריים או סודות עסקיים (להלן – "חלקים סודיים"), יציין במפורש בסעיף זה מהם החלקים הסודיים.

ג. מציע שלא ציין מהם החלקים הסודיים שבהצעתו יראוהו כמי שמסכים למסירת ההצעה כולה לעיון מציעים אחרים, אם יוכרז כזוכה במכרז.

ד. ציון חלקים בהצעה כסודיים מהווה הודאה בכך שמבחינת המציע חלקים אלה בהצעה סודיים גם בהצעותיהם של מציעים אחרים, ומכאן שהמציע מוותר מראש על זכות העיון בחלקים אלה של הצעות מציעים אחרים.

ה. יודגש כי הודעת מציע כאמור לעיל תהווה רק אחד ממכלול השיקולים בנדון שכן ההחלטה באלו חלקים של ההצעה הזוכה אין לאפשר עיון, שכן הם עלולים לחשוף סודות מקצועיים או סודות מסחריים, מסורה לשיקול דעתה של ועדת המכרזים ושלה בלבד, וכי הועדה תפעל בנושא זה בהתאם לדיני המכרזים, לדיני העיון ולאמות מדה מקובלות.

ו. החליטה ועדת המכרזים לאפשר עיון בחלקים המפורטים בהצעת הזוכה למרות שהזוכה הגדירם כסודיים, תיתן על כך ועדת המכרזים התראה לזוכה, ותאפשר לו להשיג על כך בפניה בתוך פרק זמן ההולם את נסיבות העניין.

ז. החליטה ועדת המכרזים לדחות את ההשגה, תודיע על כך ועדת המכרזים למציע הזוכה בטרם מסירת החומר לעיונו של המבקש.

ח. מבלי לגרוע מהאמור לעיל, יודגש כי שמו וכתובתו של המציע, ניסיונו ולקוחותיו לא יהוו סוד מסחרי או סוד עסקי, וזאת בכפוף לאמור בגוף המכרז. מציע שבחר להשתתף בהליך המכרז מביע בכך את הסכמתו לאמור בסעיף זה.

1.5 אופן המענה

א. בהגשת הצעתו מאשר המציע כי קרא את כל תנאי המכרז ודרישותיו, כי הבין אותם, וכי הוא מתחייב למלא אחר כל התנאים והדרישות של המכרז, ההצעה וההסכם, בדייקנות, ביעילות, במומחיות ובמיומנות, לשביעות רצון ועדת המכרזים, ובמועדים אשר ייקבעו על ידה, והכל בכפוף להוראות המכרז וההסכם.

ב. בכל מקרה בו נדרש בנוסח הסעיף פירוט כל שהוא יש למלא בדייקנות אחר הנדרש.

החתימה על ההצהרה המצורפת כנספח 1.6.6 ס"ק 2 – תצהיר כללי/הסכמה לדרישות המכרז, מעידה על כך שהמציע קרא והבין את כל התנאים והדרישות המנוסחים במכרז על סיווגם וכי הוא מתחייב, אם יזכה, למלא אחר כל התנאים והדרישות ללא סייג.

ג. יש לספק מענה במסמך Ms-Word לכל סעיף לפי המפתח הבא:

תיוג סעיף	מענה נדרש
I	סעיף מידע – יש לכתוב במענה לסעיף "קראתי והבנתי, מקובל עלי"
M	סעיף חובה – יש לכתוב במענה לסעיף "המציע יעמוד באופן מלא בדרישות הסעיף"
S	סעיף המחייב תשובת הספק לאופן העמידה בדרישה לרבות דוגמאות והרחבות– ניתן בנוסף לספק נספח טכני
O	סעיף אופציונלי – "נתמך כנדרש"
G	סעיף אופציונלי – "נתמך כנדרש + פירוט" - ניתן בנוסף לספק נספח טכני

ד. רשימת סעיפי חובה (סעיפים בעלי תיוג M)

מכלול	סעיף	תיאור
1	1.3.4	מסירת ההצעות
2	1.6.4	דרישות סף מקצועיות מהמציע
3	1.6.4.1	דרישות קדם של נותן שירותים - ניסיון בטיפול באירועים

4	1.6.4.2	דרישות קדם של נותן שירותים- מיומנות, כ״א, הסמכות, מחקר
5	1.6.4.4	דרישות SLA בפיזור גיאוגרפי– **CA1, NA1, SA1** (אזורים נוספים בסיווג S -פירוט בהמשך).
6	1.6.9	אישור רו״ח על היעדר הערת עסק חי בדוחות הכספיים של המציע
7	1.6.10	ריכוז אישורים ומסמכים שנדרש לצרף להצעה
8	3.1	מכלול השירותים (מכלול חובה)
9	3.1.7	השתתפות בסימולציות
10	3.1.8	בנייה ותחזוקת ״תיק אתר״ IR - תכולות, נכסים, מידע רלוונטי
11	3.1.9	שיתוף פעולה עם צוותי IR/מו״מ אחרים
12	3.1.10	דוחות וישיבות היגוי
13	3.1.11	סודיות, תקשורת ודוברות
14	6.1	צוות IRT
15	6.2	עדכון על שינוי ציוות/מצבת כ״א
16	7.2	בניית IR Playbook
17	7.7	תיעוד אירוע ותהליכים
18	7.9	איסוף וגיבוי עדויות פורנזיות

1.6 תנאי סף להשתתפות במכרז ואישורים שעל המציע להמציא עם הגשת ההצעה

1.6.1 כללי

א. במכרז רשאים להשתתף רק מציעים העונים במועד הגשת ההצעה על כל התנאים המפורטים בסעיף 1.6. מציע או הצעה שאינם עומדים בכל התנאים – יפסלו.

ב. במקרה של הצעה הכוללת קבלני משנה על כל קבלני המשנה לעמוד בדרישות הקדם המפורטות בסעיפים: 1.6.2, 1.6.3, 1.6.5 ולהמציא לכך אישורים כנדרש במכרז.

ג. תנאי סף המתייחסים למציע צריכים להתקיים במציע עצמו (למעט סעיף 6.1). קיום תנאי סף בתאגיד קשור (לדוגמה – חברה אם, חברה בת או חברה אחות), בארגון של המציע , בבעל מניות או בכל גורם אחר לא ייחשב כעמידה בתנאי הסף, אלא אם נאמר במפורש אחרת. המציע יוכל להיעזר בקבלני משנה לצורך עמידה בדרישות סעיף 6.1 .

1.6.2 מעמדו המשפטי של המציע

א. כתנאי מוקדם להשתתפות במכרז, על המציע להיות במועד הגשת ההצעה: תאגיד הרשום בישראל על פי דין, שאינו בעל חוב בגין אגרה שנתית למרשם הרלוונטי לשנים הקודמות לשנת 2023, ואם הוא חברה – הוא אינו בעל רישום כחברה מפרת חוק או בעל התראה לפני רישום כאמור.

ב. על המציע לצרף להצעה אישורים כמפורט בנספח 1.6.2 למכרז:

1. העתק מאומת על ידי עו״ד של תעודה תקפה המעידה על רישום המציע כתאגיד בישראל במרשם על פי הוראות הדין הנוגעות לעניין.

2. נסח רישום תאגיד עדכני לשנת 2023. נסח כאמור ניתן להפיקו באתר האינטרנט של רשות התאגידים: www.taagidim.justice.gov.il, תחת הקישור ״הפקת נסח חברה״.

3. אישור עו״ד בדבר זהות מורשי החתימה אצל המציע.

1.6.3 עמידה בהוראות חוק עסקאות גופים ציבוריים ושמירה על דיני עבודה

כתנאי מוקדם להשתתפות במכרז, על המציע לעמוד בהוראות חוק עסקאות גופים ציבוריים, תשל״ב – 1976. על המציע לצרף בנספח 1.6.3 את המסמכים הבאים:

א. עותק מאומת על ידי עורך דין של אישור תקף על ניהול פנקסי חשבונות ורשומות לפי חוק עסקאות גופים ציבוריים (אכיפת ניהול חשבונות ותשלום חובות מס), תשל״ו-1976, וכל אישור אחר הנדרש על-פי חוק זה.

ב. תצהיר מאומת ע״י עו״ד בדבר היעדר הרשעות בעבירות לפי חוק עובדים זרים, תשנ״א – 1991, ולפי חוק שכר מינימום, תשמ״ז – 1987, כמפורט בנספח 1.6.3

1.6.4 דרישות סף מקצועיות מהמציע (M)

המציע יצרף להצעתו את נספח 1.6.4 מאומת על ידי עורך דין של המציע, בדבר עמידתו בכל תנאי הסף הבאים:

1.6.4.1 דרישות קדם של נותן שירותים - ניסיון בטיפול באירועים (M)

הספק נדרש להיות ארגון שירותי IR/IRT עם ניסיון מוכח במתן שירותי IR/IRT לארגונים גדולים וניסיון מוכח בניהול, הכלה והתאוששות מאירועי סייבר מורכבים (יש לפרט היסטוריית אירועים גם מבלי לחשוף שם לקוח).

<u>דרישות קדם:</u>

- מספר לקוחות פעילים בשירות IRT/IR: **10** (יש לצרף רשימת לקוחות ורשימת אנשי קשר)
- ניסיון מוכח בניהול אירוע סייבר משמעותי: **12** אירועים בשנתיים האחרונות, מתוכם לפחות **2** אירועי סחיטה/כופרה (יש לפרט רשימת אירועים, ניתן לצרף טופס סודיות כשלב מקדים).
- ניסיון מוכח בכתיבת IR Playbook עם לפחות 15 תרחישים – **6** לקוחות, יש לספק דוגמא מושחרת, רשימת לקוחות ואנשי קשר.

1.6.4.2 דרישות קדם של נותן שירותים- מיומנות, כ״א, הסמכות, מחקר (M)

על המציע לכלול בהצעתו פרטי ראש צוות, סגן ראש צוות וחברי צוות תגובה העונים לקריטריונים המפורטים להלן -

תפקיד	שנות ניסיון	מיומנות
ראש צוות תגובה	איש אבטחת מידע עם ניסיון של 7 שנים לפחות באפיון תהליכים ובתגובה לאירועי סייבר וכופרה בפרט. ניסיון של 3 שנים לפחות בתפקיד מחקר סייבר/אנליסט בכיר (לפחות T3) ניסיון של 2 שנים לפחות בתפקיד ראש צוות תגובה	בעל ניסיון מוכח ומעורבות בתהליכי ניהול אירועי סייבר וכן ניסיון מוכח בסיוע בהתאוששות לאחר התרחשות אירוע כופרה, במהלך 3 השנים האחרונות. יכולת התנהלות מול מנהלים בכירים והצגת ממצאים והמלצות תוך כדי אירוע פעיל. קריאה/כתיבה ודיבור בעברית/אנגלית ברמה גבוהה. ניסיון בניהול צוות תגובה. ניסיון בעבודה תחת לחץ. ניסיון בעבודה בסביבת ענן. ניסיון בביצוע חקירה בהתאם לנהלי פורנזיקה ושימור ראיות ניסיון בחקירת רכיבי תקשורת לרבות נתבים, מתגים, ציוד FW, ציוד WAF.

		ניסיון בביצוע חקירות בסביבת WINDOWS , AD, EXCHANGE ו Linux ניסיון בביצוע חקירות בסביבת מסדי מערכות אחסון וגיבוי ניסיון בביצוע חקירות בסביבת מסדי נתונים. ניסיון בטיפול באירועי Ransomware. ניסיון בכתיבת נהלי תגובה לאירועי בטחון מידע והגנה בסייבר. ניסיון בביצוע חקירות בסיבות BIG DATA ומערכות SIEM. ניסיון בחקירת סביבות VIRTUALIZATION וסביבות Containers.
סגן ראש צוות תגובה	איש אבטחת מידע עם ניסיון של 5 שנים לפחות באפיון תהליכים ובתגובה לאירועי סייבר וכופרה בפרט. ניסיון של 2 שנים לפחות בתפקיד מחקר סייבר/אנליסט בכיר (לפחות T3)	בעל ניסיון מוכח ומעורבות בתהליכי ניהול אירועי סייבר וכן ניסיון מוכח בסיוע בהתאוששות לאחר התרחשות אירוע כופרה, במהלך 3 השנים האחרונות. קריאה/כתיבה ודיבור בעברית/אנגלית ברמה גבוהה. ניסיון בניהול צוות תגובה. ניסיון בעבודה תחת לחץ. ניסיון בעבודה בסביבת ענן ניסיון בביצוע חקירה בהתאם לנהלי פורנזיקה ושימור ראיות ניסיון בחקירת רכיבי תקשורת לרבות נתבים, מתגים, ציוד FW, ציוד WAF ניסיון בביצוע חקירות בסביבת WINDOWS , AD, EXCHANGE ו Linux ניסיון בביצוע חקירות בסביבת מסדי נתונים ניסיון בביצוע חקירות בסביבת מסדי מערכות אחסון וגיבוי ניסיון בטיפול באירועי RANSOMWARE ניסיון בכתיבת נהלי תגובה לאירועי בטחון מידע והגנה בסייבר. ניסיון בביצוע חקירות בסיבות BIG DATA ומערכות SIEM ניסיון בחקירת סביבות VIRTUALIZATION וסביבות Containers
חבר צוות תגובה	איש אבטחת מידע עם ניסיון של 3 שנים בתגובה לאירועי סייבר, איסוף נתונים, חקירה, מיון וביצוע פעולות ניסיון של 2 שנים לפחות בתפקיד אנליסט (לפחות T2)	בעל ניסיון מוכח במענה לאירועי סייבר, איסוף מידע, חקירה, בלימה, אכיפה וסיוע בהתאוששות. ניסיון בעבודה תחת לחץ. ניסיון בעבודה בסביבת ענן ניסיון בביצוע חקירה בהתאם לנהלי פורנזיקה ושימור ראיות הכרות עם מיומנויות ומתודולוגיות חקירה פורנזית

		ניסיון בחקירת רכיבי תקשורת לרבות נתבים, מתגים, ציוד FW, ציוד WAF ניסיון בחקירות בסביבת AD , WINDOWS, EXCHANGE ניסיון בביצוע חקירות בסביבת מסדי נתונים ניסיון בטיפול באירועי Ransomware ניסיון בכתיבת נהלי תגובה לאירועי בטחון מידע והגנה בסייבר. ניסיון בביצוע חקירות בסיבות BIG DATA ומערכות SIEM ניסיון בחקירת סביבות VIRTUALIZATION וסביבות Containers

- עבור כל עובד שהספק מציע (בעצמו או דרך ספק משנה) יצורף קובץ קורות חיים מפורט הכולל פירוט על תפקידו במענה לאירועים שונים.
- מחב״א שומרת לעצמה את הזכות לראיין אישית מועמדים. פסילת מועמד תחייב הצגת חלופה לאותו תפקיד או פסילת הספק.
- מחב״א שומרת לעצמה את הזכות לבצע בדיקות אמינות/נאותות לכל מועמד שמציע הספק.

1.6.4.3 דרישות קדם של נותן שירותים - פריסה גיאוגרפית (S)

הספק צריך להיות בעל פריסה גיאוגרפית או זמינות גיאוגרפית באופן שיוכל לעמוד בדרישות ה SLA המפורטות להלן. חריגה מ SLA תטופל באופן המפורט בהסכם.

על הספק לקחת בחשבון שחלק מהמוסדות כוללים קמפוסים הנמצאים בנקודות גיאוגרפיות מרוחקות וייתכן צורך לתגובה ומענה בו-זמנית לאזורים גיאוגרפים שונים.

על הספק לפרט איך הוא עומד בדרישות/נערך לעמידה בדרישות הפריסה הגיאוגרפית בכלל ובפרט בתנאי ה SLA לרבות התייחסות למיקום עובדים ומשרדים, ניידות וכו׳.

1.6.4.4 דרישות SLA בפיזור גיאוגרפי

אזור גיאוגרפי	זמן תגובה לפתיחת אירוע (נקודת זמן T1)	זמן תגובה הגעה לאתר/ים
CA1 (M) NA1(M) SA1(M)	מידי – 365X7X24	365X7X24 3 שעות + T1
EX1 (S)	מידי – 365X7X24	365X7X24 5 שעות + T1
EX2(S)	מידי – 365X7X24	365X7X24 7 שעות + T1

1.6.5 תצהיר בדבר היעדר ניגוד עניינים

א. תנאי מוקדם להשתתפות במכרז הינו שלמציע, לא ידוע על תפקידים, התקשרויות ועניינים שעלולים להעמידו – במקרה שיזכה במכרז - במצב של חשש לניגוד עניינים.

ב. המציע יצרף להצעתו תצהיר בנוסח המפורט בנספח 1.6.5 למכרז, בדבר היעדר ניגוד עניינים כאמור.

1.6.6 תצהיר כללי

כתנאי מוקדם להשתתפות במכרז על המציע לצרף להצעה תצהיר חתום בפני עורך-דין בנוסח המפורט בנספח 1.6.6 למכרז והכולל: הסכמה לדרישות המכרז, הצהרה על שימוש בתוכנות מקוריות וזכויות קניין, הצהרה בנוגע לאבטחת מידע והצהרה בדבר אי תיאום הצעות במכרז.

1.6.7 תצהיר בדבר העסקת אנשים עם מוגבלות

על המציע לצרף להצעתו תצהיר מאומת ע"י עו"ד בדבר העסקת אנשים עם מוגבלות, בהתאם לחוק שוויון זכויות לאנשים עם מוגבלות, תשנ"ח – 1998, כמפורט בנספח 1.6.7

1.6.8 תצהיר בדבר זמינות מיידית

על המציע לצרף תצהיר מאומת ע"י עו"ד בדבר זמינותו המיידית וזמינות המועמדים מטעמו לספק את השירותים נשוא מכרז זה, לרבות עמידה בדרישות הטכנולוגיות המפורטות במסגרת פנייה זו, כמפורט בנספח 1.6.8.

1.6.9 תצהיר בדבר העדר תביעות והליכי פשיטת רגל (M)

א. על המציע לצרף תצהיר מאומת ע"י עו"ד לפיו בעלי השליטה ומנהליו הבכירים של התאגיד נעדרים הרשעה ו/או חקירה בעבירה שיש עמה קלון או בעבירה שנושאה פיסקאלי, כגון אי העברת ניכויים, אי דיווח לרשויות המס, אי מתן קבלות רשמיות וכיו"ב, או שחלפה תקופת ההתיישנות לגבי עבירה כאמור, לפי חוק המרשם הפלילי ותקנות השבים, התשמ"א-1981, כמפורט בנספח 1.6.9.

ב. על המציע לצרף להצעתו תצהיר מאומת ע"י עו"ד, כי לא מתנהלות תביעות נגד המציע והוא אינו נמצא בהליכי פשיטת רגל ו/או פירוק שעלולים לפגוע בתפקודו ככל שיזכה במכרז, כמפורט בנספח 1.6.9.

1.6.10 אישור רו"ח על היעדר הערת עסק חי בדוחות הכספיים של המציע (M)

על המציע לצרף אישור רו"ח המאשר בדוחות הכספיים של המציע לשנים 2019-2021 לא נכללה הערת עסק חי בהתאם לכללים החשבונאיים.

1.6.11 ריכוז אישורים ומסמכים שנדרש לצרף להצעה (M)

סעיף	שם אישור/מסמך	סימון ✓ שצורף
1.6.2	תצהיר על מעמדו המשפטי של המציע	
1.6.2	תעודת רישום המציע כתאגיד בישראל	
1.6.2	נסח רישום תאגיד עדכני לשנת 2023	
1.6.2	אישור עו"ד בדבר זהות מורשי החתימה אצל המציע.	
1.6.3	עותק מאומת על ידי עורך דין של אישור תקף על ניהול פנקסי חשבונות.	
1.6.3	תצהיר מאומת ע"י עו"ד בדבר היעדר הרשעות בעבירות לפי חוק עובדים זרים	
1.6.4	תצהיר בדבר ניסיון המציע ו/או קבלני משנה הכלולים בהצעתו	
1.6.5	תצהיר בדבר היעדר ניגוד עניינים	
1.6.6	תצהיר כללי	
1.6.7	תצהיר בדבר העסקת אנשים עם מוגבלות	
1.6.8	תצהיר בדבר זמינות מיידית	
1.6.9	תצהיר בדבר העדר תביעות והליכי פשיטת רגל	
1.6.10	אישור רו"ח על היעדר הערת עסק חי בדוחות הכספיים של המציע	

1.7 בדיקת ההצעות והערכתן

המציע לא ישנה דבר ממסמכי המכרז בכל דרך, לרבות ע"י מחיקה, השמטה, תוספת, תיקון או הסתייגות, בין במסמכים עצמם ובין במכתב נפרד, ואם יעשה זאת תהיה ועדת המכרזים רשאית, לפי שיקול דעתה המוחלט והבלעדי, לפסול את הצעתו של המציע או להתעלם מכל שינוי כאמור ולראות בהצעת המציע כהצעה בלתי מסויגת; במקרה של אי הצגת מחיר ו/או שיעור הנחה ליד סעיף כל שהוא תהיה ועדת המכרזים רשאית לפנות למציע בשאלת הבהרה או לראות כאילו המחיר כלול ביתר הסעיפים. במקרה של סטייה עקב טעות אריתמטית בין המחיר ליחידה לבין מכפלת המחיר ליחידה במספר היחידות, המחיר שייקבע הינו המחיר ליחידה.

א. אופן שקלול ההצעות

הליך בחירת הספק הזוכה/הספקים הזוכים יתבצע באופן הבא:

1. בדיקת עמידת ההצעות בתנאי הסף.

ועדת המכרזים – או מי שזו תמנה לצורך כך - תבחן האם המציע עומד בתנאי הסף המפורטים במסמכי המכרז. מינתה הועדה גורם לבחינת העמידה בתנאי הסף יהיו ממצאיו טעונים את אישורה. רק מציע שיעמוד בכל תנאי הסף יעבור לשלב בדיקת האיכות. מציעים אשר לא יעמדו בכל תנאי הסף, יקבלו ציון "נפסל" ותועבר להם הודעה על כך.

2. ועדת המכרזים הסמיכה ועדת משנה לבדיקת איכות מעני המציעים "ועדת המשנה". להלן הרכב וועדת המשנה:

- רו"ח אפרת פיינשניידר – יו"ר הוועדה, מנהלת כספים ומנהל, מחב"א
- תומר נורי – יועץ חיצוני למחב"א
- רוני סולומון, מנהל אבטחת מידע והגנת הפרטיות, אונ' בר אילן
- אלירן סולמון, ראש מנהל אבטחת מידע, אונ' אריאל
- חנן רודניק – מנהל תשתיות ואבטחת מידע, מחב"א

3. בדיקת איכות ההצעות תבוצע על ידי ועדת המשנה בהתאם למפ"ל ניקוד איכות המפורט בנספח 1.7. הכולל רשימת קריטריונים לבחינה ומשקל יחסי בגין כל קריטריון. מובהר בזאת כי לצרכי ניקוד האיכות של ההצעה רשאית ועדת המשנה או וועדת המכרזים לזמן את המציעים להציג את הצעותיהם, כפי שהוגשו, וזאת בהודעה שתישלח לפחות שבוע מראש. **ציוני האיכות שינתנו על ידי ועדת המשנה יהיו טעונים אישור של ועדת המכרזים שתהיה רשאית להכניס בהם שינויים.**

4. רק ההצעות אשר עמדו בציון סף איכות של 70% יעברו לשלב הבא. הצעות שיקבלו ציון נמוך יותר יפסלו . במידה ותוגש הצעה אחת בלבד ציון למעבר לשלב הבא ירד ל-60%. **מעטפות המענה הכספי של המציעים שיעמדו בציון סף האיכות יפתחו רק לאחר אישור ציוני האיכות על ידי ועדת המכרזים.**

5. לאחר אישור ועדת המכרזים את ציוני האיכות, ייפתחו מעטפות המענה הכספי של המציעים שיעמדו בציון סף האיכות , ותשוקלל הצעת המחיר שהוגשה על ידי המציע.

6. שיקלול של הצעת המחיר יתבצע באופן הבא:

A1 – מחיר התנעה למוסד בינוני

B1– מחיר ריטיינר ל 3 שנים למוסד בינוני

C – מחיר שעות עבודה לפני השעה ה – 300

A2 – מחיר התנעה למוסד גדול

B2 – מחיר ריטיינר ל 3 שנים למוסד גדול

עלות = A1*0.5+0.5*B1+0.5*A2+0.5*B2+C*300

את מלוא הניקוד (ציון 100) תיתן ועדת המכרזים למציע(ים) עם סך העלות (כפי שחושבה לעיל) הנמוכה ביותר. שאר המציעים יקבלו ניקוד באופן יחסי.

7. יחס עלות תועלת יחושב כסכום של:

- איכות (תועלת) - יהווה 50% מהציון המשוקלל של המציע.
- מחיר (עלות) - יהווה 50% מהציון המשוקלל של המציע.

ב. אופן בחינת ניסיון המציע:

1. ועדת המשנה תהיה רשאית לפנות לאנשי הקשר (לכולם או לחלקם) ולגורמים אחרים על פי שיקול דעתה כחלק מהליכי קביעת ניקוד האיכות.
2. הפנייה לאנשי קשר ואחרים אפשר שתכלול בין היתר קבלת חוות דעתם לרמת שירות, זמינות, שביעות רצון משירותי המציע ועוד. על המציע להביא בחשבון את האמור לעיל ולציין בטבלה את הלקוחות המתאימים ביותר.
3. ועדת המכרזים תהיה רשאית להתחשב בניסיון הנצבר במחב"א או במוסדות בהתקשרויות קודמות עם המציע ככל שהיו.

ג. הצעה זוכה תהה זו שתקבל ציון משוקלל איכות ומחיר גבוה ביותר.

ד. ועדת המכרזים רשאית אך לא חייבת על פי שיקול דעתה לבחור יותר מהצעה זוכה אחת.

ה. לכל מוסד תהיינה 3 אופציה לעבוד מול הספק/ים הזוכ/ים:

- עבודה על בסיס בנק שעות באופן מלא (ניתן לאפשר התנעה כמחיר קבוע מראש לפי התמחור המכרז).
- תשלום מחיר התנעה, תשלום ריטיינר קבוע שנתי ותוספת שעות עבודה לפי הצורך (אך ורק בגין שירותים בעולמות ה IRT שאינם כלולים בתכולת המכרז).
- עבודה במודל משולב של ריטיינר ושעות .

בכל מודל עבודה המציע הזוכה יהיה מחויב בכל ההתחייבויות הנובעות מהמכרז (לרבות SLA, פריסה גאורגרפית וכו').

1.8 תוקף ההצעה

ההצעה למכרז תהיה בתוקף בהתאם למופיע בסעיף 1.1.2 - טבלת ריכוז מועדי המכרז, בשורה "מועד תוקף ההצעה".

המציע יאריך את תוקף ההצעה, לבקשת מחב"א, עד לקבלת החלטה סופית של זכייה במכרז זה.

1.9 הסכם התקשרות חתום בראשי תיבות

המציע יחתום על הסכם ההתקשרות המצורף להלן כנספח 1.9. ההסכם ייחתם בראשי תיבות על ידי מורשה/י החתימה של המציע ויוחתם בחותמת התאגיד בכל עמוד מעמודיו וכן בחתימה מלאה ובחותמת התאגיד במקום המיועד לכך בסוף ההסכם.

חתימה זו מעידה על הסכמת המציע לתנאי ההסכם. השלמת החתימות והפרטים כגון עדכון ההסכם בעקבות מענה לשאלות הבהרה והגשת נספחים (ערבות ביצוע, ביטוח וכדומה), תעשה בתוך 30 יום מיום הכרזת ועדת המכרזים על המועמד להיות הספק הזוכה.

1.9.1 מועד כניסת ההתקשרות לתוקף

מועד כניסת ההתקשרות לתוקף מותנה בהשלמות האמורות בסעיף 1.9 לעיל, עם השלמת החתימות והפרטים המועמד להיות הספק הזוכה יוכרז כספק הזוכה בפועל.

1.10 זכויות עורך המכרז (I)

1.10.1 ביטול המכרז

ועדת המכרזים של מחב״א רשאית על פי שיקול דעתה המוחלט והבלעדי, לבטל את המכרז או לפרסם מכרז חדש במקומו. אם המכרז יבוטל לפני בחירת הזוכה, ההודעה על ביטולו תישלח לכל המציעים אשר הגישו הצעות למכרז.

במקרה של ביטול המכרז, לא יינתן פיצוי למציעים בכל צורה שהיא.

1.10.2 שאלות הבהרה

ועדת המכרזים ו/או מי שיוסמך מטעמה רשאית לבקש מכל מציע, בכל שלב של הליך המכרז, הבהרות בכתב או בעל פה להצעה כולה או מקצתה, ובלבד שלא יהיה בכך כדי לאפשר למציע לשנות את הצעתו או להעניק לו יתרון בלתי הוגן על מציעים אחרים. ההבהרות יהיו חלק בלתי נפרד מההצעה.

ועדת המכרזים ו/או מי שיוסמך מטעמה רשאית לדרוש מכל מציע השלמת מידע חסר, המלצות או אישורים המתייחסים לדרישות המפורטות במכרז, לצורך בחינת עמידתו של המציע בתנאי המכרז, וכן לבצע כל פעולה אחרת הדרושה לבחינת ההצעה, לרבות ביקור במתקני המציע.

ועדת המכרזים ו/או מי שיוסמך מטעמה רשאית להורות על תיקון פגם שנפל בהצעה או להבליג על הפגם, אם מצאה כי אין בכך כדי לפגוע בשוויון בין המציעים וכי החלטה זו משרתת באופן המרבי את טובת מחב״א ואת תכליתו של מכרז זה.

1.10.3 פסילת הצעה

המציע מתחייב שלא לתאם מחירים / הצעות עם מציעים אחרים, ולא לבוא בהסדרים עם מציעים פוטנציאליים אחרים. המציע מצהיר כי הוא מודע לכך שכל פעולה בניגוד לאמור לעיל עלולה להוות עבירה פלילית בין היתר בהיותה בגדר הסדר כובל.

וועדת המכרזים של מחב״א תהיה רשאית על פי שיקול דעתה המוחלט לפסול הצעות בהן קיים לדעתה חשש לתאום פסול כאמור.

ועדת המכרזים שומרת לעצמה את הזכות לפסול הצעה, בין היתר, בגין המקרים הבאים:

א. הצעה מסויגת או מותנית

- מציע לא יסייג את הצעתו או יתנה אותה באופן שאינו עולה בקנה אחד עם דרישות המכרז, ובכלל זה ימנע מכל שינוי, הסתייגות או התניה על דרישות ההסכם ונספחיו.
- מציע הסבור כי דרישות המכרז ראויות להתניה או להסתייגות, רשאי להעלות את השגותיו או את הערותיו במסגרת הליך ההבהרות בלבד. וועדת המכרזים תשקול את פנייתו ותשיב לו, הכול בהתאם לקבוע בסעיף 1 לעיל. אין להסתייג או להשיג על תנאי ההליך במסגרת ההצעה גופה.

ב. הצעה שהיא לדעת הועדה בלתי סבירה או הצעה שחסרה בה התייחסות מפורטת לסעיף מסעיפי המכרז שלדעת ועדת המכרזים מונע הערכת ההצעה כדבעי. ככל שמוצאת הועדה לנכון לפסול הצעות כאמור, תעניק הועדה למציע את הזכות לטעון טענותיו בכתב בטרם קבלת החלטה סופית בסוגיה.

ג. הצעה תכסיסנית - הצעה שלדעת הועדה כוללת מידע מטעה או הצעה הלוקה בחוסר תום לב. ככל שמוצאת הועדה לנכון לפסול כאמור, תעניק הועדה למציע את הזכות לטעון טענותיו בכתב בטרם קבלת החלטה סופית בסוגיה.

1.10.4 היקף ההתקשרות

מחב״א תהיה רשאית להגדיל את היקף ההתקשרות במכרז בכל עת או להקטין את היקף ההתקשרות מול הספק הזוכה על פי תנאי המכרז והכול עפ״י שיקול דעתה הבלעדי.

1.11 הצעת הספק

1.11.1 מבנה כללי

א. מבנה ההצעה יהיה תואם באופן מלא לדרישות המכרז. חובה לענות לפי המבנה והפירוט שבכל סעיף. ועדת המכרזים תהיה רשאית לפסול הצעה אשר תוגש שלא במבנה זה או לא תהיה שלמה, וזאת על פי שיקול דעתה המוחלט והבלעדי.

ב. נספחי המכרז מהווים חלק בלתי נפרד ממסמכי המכרז. עם זאת, במקרה של סתירה בין נספחי המכרז לבין גוף המכרז יגבר האמור בגוף המכרז.

ג. תוכן ומבנה ההצעה בכל רכיב (סעיף ותת סעיף) יתאים לסעיף המקביל במכרז. המציע רשאי להוסיף בנושאים טכניים בלבד הערות והצעות משלו. במקרה של הצעה ארוכה יש להפנות לנספח בסוף ההצעה שיסומן במספר הרכיב המפנה. השימוש בנספחים יהיה על מנת לפשט את גוף ההצעה ולהקל על קריאתה. חומר מקצועי ופרסומי יצורף כנספח לסעיף הרלוונטי ויסומן כמפורט לעיל.

ד. מסמכים שהמציע יצרף ושאינם מהווים חלק מדרישות המכרז יצורפו כשהם מתויקים בכריכה נפרדת (תיק, קלסר) והם מסומנים בהתאם לסעיף הרלוונטי.

ה. יובהר, כי ועדת המכרזים אינה מחויבת להתחשב בדפים, חוברות, DoK, מצגות וכד', שאינם נדרשים במפורש או שהגשתם לא הותרה במפורש.

1.11.2 מספר עותקים

ההצעה למכרז תוגש בעותק מודפס כולל מדיה (Disk-On-KEY).

בהצעה - העמוד הראשון (על כל מסמכיו, נספחיו והאישורים המצורפים) יוחתם בחותמת התאגיד של המציע ובחתימה מלאה של מורשי החתימה המוצהרים. ביתר העמודים, ניתן לחתום בראשי תיבות בחתימת מורשי החתימה כאמור.

המציע ידביק על הצד החיצוני של הצעת המקור, מעטפה סגורה היטב, ללא פרטי המציע על גבה, ובתוכה יופיעו שם המציע ופרטי איש קשר מטעמו (מספר טלפון וכתובת) לשם החזרת המעטפה במקרה הצורך.

ההצעה תוגש ארוזה באריזה אחת שעליה ירשם **"מכרז פומבי מספר 2-2023 שירותי IR\IRT למחב"א והמוסדות האקדמאים החברים בה"** ובתוכה 2 מעטפות שתכולתן תהייה כדלהלן:

1. מעטפה ראשונה: (תסומן "פרק 1 - מנהלה")

המעטפה תכלול את מענה המציע **לכל** דרישות המכרז **פרט** להצעת המחיר כשמענה זה לפרק כרוך ומוחתם עפ"י המצוין לעיל.

כמו כן, המעטפה תכלול DoK עם כל המסמכים שבמעטפה. המענה יכלול מסמכי מקור בפורמט PDF.

2. מעטפה שנייה: (תסומן כ"הצעת מחיר")

המעטפה תכלול את עותק מודפס של נספח 11 כשהוא ממולא וחתום באופן האמור לעיל.

כמו כן, המעטפה תכלול DoK עם כל המסמכים שבמעטפה, המענה יכלול מסמכי מקור בפורמט PDF.

ניתן, במקום זאת לחתום, במקומות האמורים לעיל, בסעיפים 1 ו – 2, בחתימה אלקטרונית ובלבד שיצורף אישור עו"ד בדבר זהות החותם וכן שהחברה הסמיכה את החותם לחתום בשמה בחתימה אלקטרונית ולחייבה בחתימה כאמור.

1.12 בעלות על המכרז ועל ההצעה (I)

1.12.1 בעלות על מסמכי המכרז והשימוש בהם

מסמכי המכרז הינם קנינה הרוחני הבלעדי של מחב"א, ומועברים למציע לצורך הגשת ההצעה בלבד. אין לעשות בהם שימוש כלשהו שאינו לצורכי הכנת הצעת המציע.

1.12.2 בעלות על ההצעה ושימוש בה

הצעת המציע (המענה לבקשה להצעות) היא רכושו של המציע. למחב״א תהא האפשרות להשתמש בהצעה ובמידע שבה לכל צורך הקשור בתהליך זה של בקשה להצעות עד להשלמת ההתקשרות.

1.12.3 חשיפת פרטי הצעה לצדדים שלישיים

א. עורך המכרז מתחייב לא לגלות היבטים רגישים מסחרית מתוכן ההצעה שקיבל לצד שלישי, זולת היועצים המועסקים על ידו, אשר גם עליהם חלה חובת סודיות.

ב. ועדת המכרזים תאפשר למציעים שלא הוכרזו כזוכה במכרז, לעיין בפרוטוקול ועדת המכרזים ובמסמכי ההצעה הזוכה על פי המוגדר לעיל בסעיף 1.4.

1.13 מחירים

א. כל המחירים שיהיו נקובים בהצעה יהיו סופיים, בשקלים, ללא מע״מ ויכללו את כל מרכיבי העלות.

ב. כל המחירים יכללו את מלוא המיסים (למעט מע״מ), ההיטלים או תוספות אחרות, לרבות כל תשלום מסוג כלשהו לצד שלישי בגין תמלוגים ו/או זכויות שימוש.

1.14 תקופת ההתקשרות

משך ההתקשרות לשירות הוא 3 שנים עם אופציית הארכה השמורה למחב״א לעד שנתיים נוספות מיום חתימה על הסכם ההתקשרות עם הספק הזוכה. למחב״א שמורה הזכות לסיים את ההתקשרות לפני תום התקופה בהתאם למפורט במסמכי המכרז ובהסכם.

1.15 היררכיה בין מסמכים, פרשנות וסמכות שיפוט

א. בכל מקרה של סתירה שאינה ניתנת ליישוב בין נוסח המכרז לבין נוסח ההסכם, יגבר נוסח ההסכם.

ב. ביטויים המופיעים בלשון יחיד משמעם גם בלשון רבים ולהיפך; ביטויים המופיעים בלשון זכר משמעם גם בלשון נקבה ולהיפך.

ג. כותרות הסעיפים במכרז ובנספחיו הן למטרות נוחות ולא ישמשו לצרכי פרשנות.

ד. סמכות השיפוט הבלעדית לדון בתובענה שעילתה במכרז זה נתונה לבית המשפט המוסמך במחוז תל-אביב.

ה. אין בסעיפי המכרז כדי לגרוע מזכויותיו של מחב״א על פי כל דין.

2. יעדים, מטרות והליכים (I)

על הזוכה במכרז לעמוד בכל היעדים והמטרות המפורטים להלן ולקיים את כל הדרישות וההליכים המפורטים בפרקים 1 עד 11 [כולל] של המכרז.

2.1 כללי

א. ההסלמה באירועי סייבר וההשפעה שלהם ברמת המדינה, ברמה העסקית וברמת הפרט מחייבת השבחה של מערכי הגנת הסייבר ומענה לאיומים ואירועי אבטחה ברמות מורכבות שונות ובאופן שתאפשר הגדלת החוסן ובמידת הצורך תאפשר הכלה והתאוששות מהירה במינימום נזק.

מתודיקה, ניסיון ומקצועיות הם תכונות הכרחיות לניהול אירוע סייבר מורכב, לגופים אקדמאים כמו לרוב הארגונים אין את הפריבילגיה או את המשאבים הנדרשים לטיפול והכלה של איום סייבר בציר הזמן ולכן כולל מכרז זה שלל שירותי IR/IRT בפריסה גיאוגרפית מלאה.

ב. המכרז הינו לאספקת שירות IR/IRT כוללים ומענה לאירועי סייבר בסביבה האקדמאית.

כחלק מפעילות היערכות לאירועי סייבר, פועלת מחב״א ליצירת תשתית מסחרית וטכנית להתקשרות עם חברות מומחות בתחום ה IR/IRT שישמשו לתמיכה בגופי אבטחת המידע במוסדות האקדמאים במקרה של אירוע סייבר. השירות הנרכש ישמש לסיוע באפיון וזיהוי איום, רישום וניהול האירוע, איסוף פורנזיקה וממצאים, בלימה, הכלה והתאוששות.

השירות יפעל בהלימה ובסנכרון מלא לגופי אבטחת המידע הפנימיים באוניברסיטאות הרלוונטיות ובקמפוסים השונים, בהתאמה למדיניות סייבר וביטחון באותם גופים ולסביבות הייחודיות הכוללות את ״החופש האקדמאי״ והאוטונומיה המתאפשרת בסביבות אלו.

אופי השירות יכלול הגעה פיזית לאתר תחת הגדרת SLA ובהתאם לנסיבות.

3. SOW – תיחום

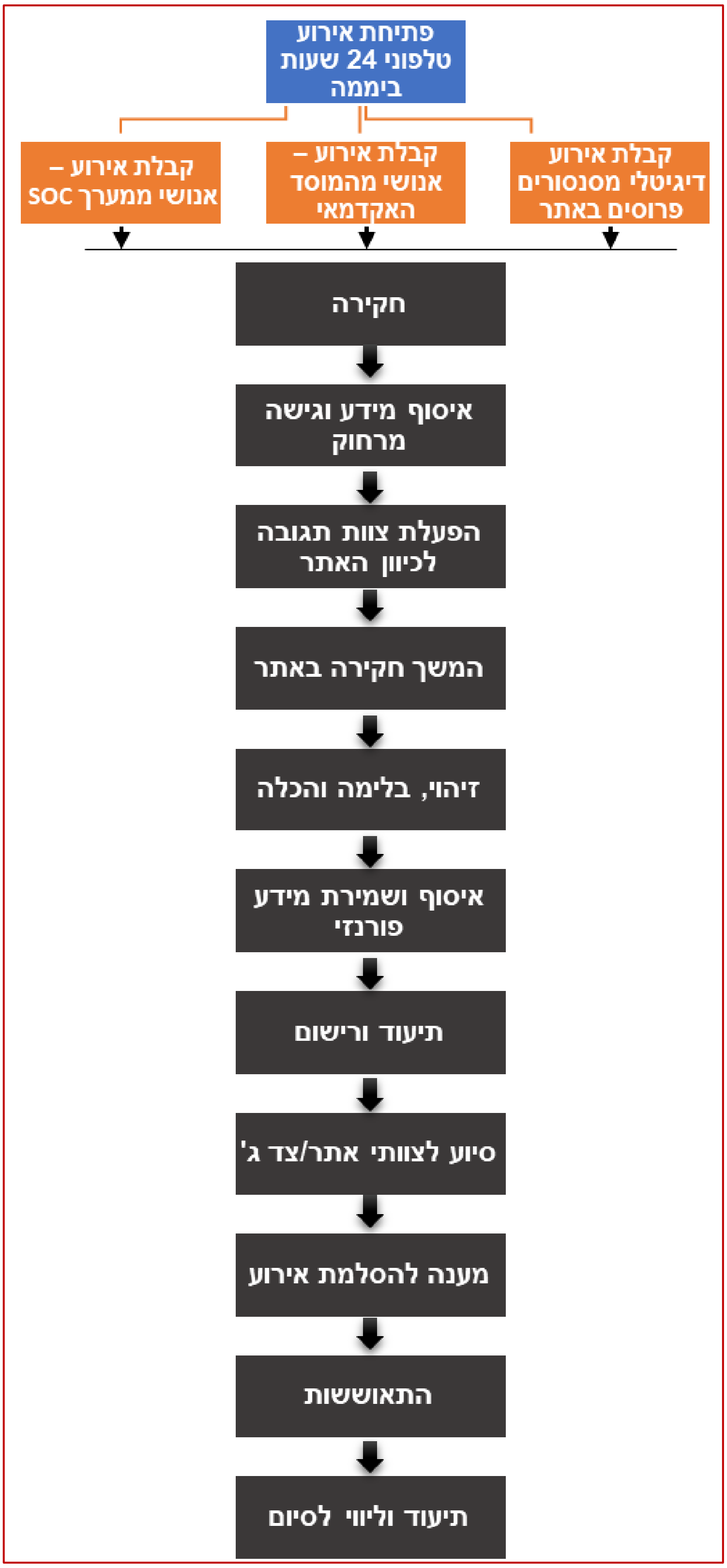
3.1 מכלול השירותים (M)

3.1.1 תכולת השירותים הנדרשת - מכלול חובה

תת מכלול	תיאור	הערות
1	ביצוע Onboarding לכל מוסד אקדמאי לרבות למידת הסביבה התקשובית	ראה סעיף 3.1.4
2	בנייה ותחזוקת ״תיק-אתר״ מעודכן	בהתאם לסעיף 3.1.8
3	השבחה של נהלים קיימים ושיטות אופרטיביות להתמודדות עם אירועי סייבר	
4	כתיבה ל IR Playbook ל 15 תרחישים	ראה סעיף 7.2
5	הקצאת מומחה IR בשילוב צוות IRT לכל מוסד אקדמאי	
6	מענה בזמן אמת לאירוע או אסקלציה של אירוע	7X24
6	הגעה לאתר כחלק משירות IRT תחת SLA	בהתאם להנחיית מנהל אבטחת מידע במוסד האקדמאי ו/או חומרת אירוע ו/או IR Playbook
7	חקירת אירוע מרגע הכרזה דרך זיהוי/עדכון ועד הכלה מלאה.	

8	הכלת אירוע וניהול צוותי תגובה ואסטרטגיית תגובה	נקיטת כל הפעולות הנדרשות לעצירה מידית (הכלה ומניעת התפשטות) של האירוע, וכן פעילות לנטרול התקיפה, להסרת הנוזקה וכיו״ב.
10	שיתוף פעולה עם חברות ניהול מו״מ	
11	סיוע בהתאוששות מאירוע עד חזרה לשגרה	
12	עבודה בסינרגיה עם גופי סייבר במוסדות האקדמאים	
13	פריסת כלי IR כשלב מקדים או בזמן אירוע	פירוט בהמשך
14	איסוף פורנזיקה וממצאים לפי מודל DFIR	פירוט בסעיף 7.9
15	תיעוד כל תהליכי ה IR לרבות פעולות IRT בשטח	
16	הפקת דוחות פוסט-אירוע וניהול ידע	
17	סיוע ביצירה והפצה של IOC וחתימות/חוקי חסימה.	
18	זיהוי חולשות/נוזקות/RCA שהובילו לאירוע	
19	זיהוי נקודת ״התפרצות״ Zero-Patient	
20	סיוע במילוי טפסי IR של מחב״א בזמן אירוע	

3.1.2 תהליך חקירה, טיפול והכלת אירוע – תיאור כללי



3.1.3 תהליך חקירה, טיפול והכלת אירוע – תהליך מפורט (S)

יש לפרט את מתודולוגית העבודה של הספק בהתאם לסעיפים להלן :

א. קבלת קריאה אנושית או דיגיטלית ופתיחת אירוע – תהליך זמין 24 שעות ביממה, 7 ימים בשבוע, 365 יום בשנה.

ב. אימות אירוע, סנכרון דיווחים, סנכרון מול צוותי סייבר של ארגון היעד לגבי מה נבדק/בוצע לשלב זה, תחילת חקירה ממוחשבת של אירוע תוך שימוש בשילוב מיידעים, איסוף מידע ממערכות קיימות או מסנסורים שהוטמעו מראש.

ג. המשך חקירה על בסיס גישה מרחוק איפה שמתאפשר בהתאם לסביבה ובאישור מנהל אבטחת המידע הרלבנטי.

ד. הפעלת צוות תגובה לכיוון האתר הרלוונטי בהתאם להגדרת SLA ובכפוף להנחיית מנהל אבטחה המידע הרלבנטי ו/או לחומרת האירוע ו/או לאסקלציה מוגדרת ב IR Playbook.

ה. הגעת הצוות לאתר, התמקמות והגדרת תוכנית פעולה ותיעדוף משימות חקירה, בלימה והכלה בהנהלת ראש צוות תגובה.

ו. בניית תיק מידע טקטי ממוקד לאירוע הכולל וקטור תקיפה מוערך, נוזקות משולבות, מערכות מושבתות ונזק תקיפה והשפעה כללית על תהליכים ותשתיות.

ז. בניית המלצות פעולה וקבלת אישור פעולה ממנהל האבטחה באתר ליישום תוך שילוב צוותי סייבר של המוסד האקדמאי ו/או צוותים חיצוניים. ביצוע בלימה בחירום על בסיס מידור תשתיות, חסימת כתובות ומזהים, חסימת משתמשים, סנכרון מודיעין.

ח. המשך חקירה במקביל להפעלת כלל הפעולות והאמצעים להכלת האירוע תוך התבססות על פרוטוקולי בלימה ואיסוף פורנזיקות לפי נוהל DFIR (מפורט בהמשך) באירועים רלוונטיים.

ט. במידת הצורך הרחבת מידור ובידוד תשתיות "נגועות", הסרת נוזקות, הפעלת חוקי מידור לסגירות וקטור התוקף.

י. במידה והאירוע מסלים לכיוון מו"מ עם תוקף או מימד האירוע גדל, צוות ה IRT בניהול ראש הצוות ישתף פעולה ויבצע פעולות תחת הנחיות שיגיעו מהגופים המוסמכים באוניברסיטה ודרכם מגופי צד ג' לרבות צוותי IR/ IRT מחו"ל, גופי אכיפה, מערך הסייבר, נציגי ביטוח סייבר, מנהל מו"מ וכו' והכל תחת הנחיות של מנהל אבטחת המידע בארגון היעד.

יא. המשך ביצוע כלל הפעולות הנדרשות להתאוששות וחזרה לשגרה תוך שמירה על ממצאים פורנזיים חיוניים.

יב. ביצוע תחקיר פוסט-אירוע לרבות מילוי דו"ח סיכום שיוגש למנהל אבטחת המידע הרלבנטי ורישום ממצאים בקובץ לוג אירוע (מפורט בהמשך), ליווי בהפצת IOC והעברת המלצות לצוותי סייבר במוסד האקדמאי.

יג. במידת הצורך ובהתאם לנסיבות השתתפות ראש צוות IRT בדיון מסכם ו/או מתן עדות בתהליך משפטי (כפוף להנחיות מנהל אבטחת מידע במוסד האקדמאי).

3.1.4 תהליך התנעה מול מוסד אקדמאי (S)

במידה ומוסד אקדמאי בוחר להשתמש בשירותיו של ספק שזכה במכרז יופעל תהליך התנעה סדור מול כל ארגון יעד. תהליך ההתנעה יכלול לפחות ראש צוות תגובה, סגן ראש צוות (אם רלוונטי לארגון היעד) ואנשי תגובה. מטרת תהליך ההתנעה הוא לבצע "On-Boarding" של ספק השירותים מול המוסד האקדמאי, מנהל האבטחה שלו (CISO) וצוות האבטחה. תהליך ההתנעה יתבסס לפחות על 3 ימי התנעה באתר הלקוח במהלכם יבדקו נהלים, יוגדרו/יועשרו תהליכי ונהלי IR, ייאסף המידע להכנת ה IR Playbook ותבוצע הכרות עם סביבת התקשוב הקיימת.

תהליך ההתנעה הוא מנדטורי לתחילת פעילות סדורה מול המוסד האקדמאי והוא השלב המקדים להכנת תיק אתר ונוהל IR – IR Playbook.

יש לפרט את מתודולוגית תהליך ההתנעה של הספק אשר יכלול בין היתר את התוצרים הבאים :

- היכרות הדדית
- הגדרת נוהל ותהליך פתיחת אירוע – אנושי ואלקטרוני

- הסכמה על אופן תקשורת/פלטפורמה מקוונת מאובטחת בעת אירוע
- בחינת נהלי אבטחה קיימים לטיפול באירוע סייבר
- איסוף מידע להכנת נוהל IR – Playbook.
- כתיבת תוכנית IR ל 15 תרחישי איום לפחות
- הכנת התשתית לחיבוריות מרחוק – אם רלוונטי.
- בניית תיק אתר

3.1.5 פריסת כלים ומנגנונים שונים (S)

הספק יכול לבחור לפרוס כלים, סנסורים ומנגנוני אבטחה כצעד מקדים למתן השירות במידה והוא מוצא לנכון לבצע זאת עקב אי מוכנות של ארגון היעד. במידה ולא בוצעה פריסה מקדימה בזמן אירוע יבוצע פריסה בחירום של כלים ומנגנונים שונים כדי לשפר יכולת חקירה וביצוע בלימת אירוע בחירום.

יש לפרט אילו כלים, סנסורים ומנגנוני אבטחה יסופקו ובאיזה שלב.

פריסת הכלים מותנית באישור מוקדם של המוסד האקדמאי. סירוב לפריסת כלים לא יתפס כעילה לאי קבלת שירות IR מהספק.

למוסד האקדמאי אופציה לרכוש שירות של פריסה קבועה של כלים ומנגנונים המפורטים בסעיף זה באופן יזום. יש לפרט בפרק התמחור האופציונלי את העלויות הרלוונטיות.

3.1.6 הדרכות והעשרות (S)

הספק יכלול בשירות ה IR/IRT הדרכות העשרה לצוותי הסייבר בארגון היעד. הדרכה תכלול לפחות 3 מפגשים שנתיים באורך מינימלי של חצי יום. ההדרכה תהיה באתר הלקוח ומוגבלת ל 15 משתתפים. הספק מוזמן להרחיב להצעות הדרכה והעשרה נוספות בפרק המסחרי תחת "הרחבות אופציונליות".

יש לפרט אילו הדרכות והעשרות יסופקו ע"י הספק ובאיזה תדירות.

3.1.7 השתתפות בסימולציות (M)

הספק יכלול בשירות ה IR/IRT השתתפות בתרגיל "אירוע סייבר משמעותי/אירוע משבר סייבר" שיבוצע על ידי גוף צד ג'. העלות לשירות ה IR/IRT תכלול השתתפות ביום תרגיל מלא. יתרה מזאת אם לספק או לשותפיו יש יכולת ביצוע סימולציות ותרגילי סייבר יש לפרט על כך בפרק "הרחבות אופציונליות".

3.1.8 בנייה ותחזוקת "תיק אתר" IR - תכולות, נכסים, מידע רלוונטי (M)

א. בניית תיק אתר

תיק אתר ייכתב ע"י הספק הזוכה עבור כל מוסד אקדמאי רלוונטי שיחליט לרכוש את השירות. תיק האתר יכלול לפחות:

- רשימת נכסים דיגיטליים רלוונטיים לרבות מזהי נכסים (ID ,HASH ,IP ,FQDN) , כלי חקירה ומקורות מידע לצורך ביצוע חקירה
- שרטוטי רשת
- רשימת בעלי הרשאות פריבילגיות וקבוצות פריבילגיות
- נהלי מענה לאירוע "משבר סייבר"
- IR Playbook – נוהל IR עדכני לרבות תהליכי אסקלציה ופרוטוקולי הכלה עדכניים.
- פרטי קשר של בעלי תפקיד רלוונטיים
- דרכי תקשורת עם בעלי תפקיד רלוונטיים
- נוהל תיוג ותיעוד אירוע
- נוהל חקירת אירוע
- נוהל DFIR עדכני.

- התייחסות לסיכונים והשפעות חקירה בנכסים המושפעים ממודל "החופש האקדמאי" כולל דרכי התמודדות בזמני אירוע
- רשימת מערכות מידע לצורך חקירת אירוע כולל מערכות תפעול וסייבר
- שמות המשתמש בעבור ביצוע החקירה -על השמות להיות בסכמה הארגונית ולא באופן שיבליט שמדובר במשתמשי IR, פרטי ההתחברות יישמרו ויועברו באופן מאובטח

ב. תחזוקת "תיק אתר" IR

תיק האתר יתוחזק ויעודכן רבעונית או בתדירות גבוהה יותר אם הנסיבות מחייבות לדוגמא לאחר שילוב מערכת הגנה אנליטית חדשה או יכולת הגנת סייבר מתקדמת, לאחר שינוי מבני או שינוי כ"א משמעותי, לאחר חקירת אירוע והכל בסנכרון ובאישור של מנהל האבטחה בארגון היעד.

נוסף על כן תבוצע בדיקה רבעונית לגישה מרחוק ושימוש בחשבונות משתמשים לצורך חקירה.

3.1.9 שיתוף פעולה עם צוותי IR/מו"מ אחרים (M)

במידה והאירוע מסלים לכיוון מו"מ עם תוקף או היקף האירוע גדל, צוות ה IRT בניהול ראש הצוות ישתף פעולה ויבצע פעולות תחת הנחיות שיגיעו מהגופים המוסמכים באוניברסיטה ודרכם מגופי צד ג' לרבות צוותי IR/IRT מחו"ל, גופי אכיפה, מערך הסייבר, נציגי ביטוח סייבר, מנהל מו"מ וכו' והכל תחת הנחיות של מנהל אבטחת המידע בארגון היעד. הספק ינחה את ראש הצוות ה IRT והוא את צוות התגובה מבעוד מועד לשתף פעולה באופן מלא מול גופי IR/IRT/מו"מ אחרים תוך שיתוף נתוני חקירה וביצוע פעולות בלימה שיתקבלו.

3.1.10 דוחות וישיבות היגוי (M)

הספק הזוכה יפיק דו"ח IR חודשי על פעולות שבוצעו וישתתף בישיבת היגוי תקופתית.

ישיבות היגוי יהיו בתדירות של אחת לרבעון למעט אם היה אירוע. במקרה זה, התדירות תיקבע על ידי מנהל האבטחה במוסד האקדמאי.

דוחות יוגשו אחת לחודש. דו"ח מסכם יוגש אחת לרבעון.

הדוח יהיה בנוי בהתאם למתודולוגיות מוכרות לרבות הדרישות במסמך זה והפרטים הבאים :

תמצית מנהלים, זמני האירוע והחקירה, timeline של האירוע, timeline של החקירה לרבות גורמים מעורבים, הפעולות שבוצעו וזמנים בפורמט תאריך ושעה, הסבר על שורש הבעיה והתקדמות התוקף, ניתוח ההשפעות על הארגון לרבות על נכסי המידע של הארגון ועל פעילותו העסקית, אופן התגובה וההכלה לרבות שינויים טכניים ומנהלתיים שבוצעו, הצעות לשיפור ברמת נהלים, תהליכים או טכנולוגיות שיאפשרו מניעה ו\או הכלה ו\או זיהוי מיטביים יותר בעתיד.

על המציע לספק דוח פוסט אירוע לדוגמא כחלק מההצעה.

3.1.11 סודיות, תקשורת ודוברות (M)

הספק הזוכה, אנשיו ואנשי ספקי משנה – אם יהיו כאלה - יחתמו על נספח סודיות כחלק מחייב של זכייה במכרז זה.

הספק מתחייב שהוא או אנשים באחריותו לא יפרסמו פריט מידע כלשהוא הקשור לפעילות IR/IRT במחב"א ובמוסדות, לא יפרסמו דעה או כל מידע בתקשורת או ברשתות חברתיות ולא יצלמו סרטונים בשטחי האוניברסיטאות ובקמפוסים השונים. כמו כן הספק לא ישתמש בהישגים, פעולות או דוקטרינות שלמד או יישם במהלך השירות לפרסום או הצגת יכולתו מול גופים אחרים.

הספק מתחייב לא להעביר מידע בערוצים פנימיים (ערוצי תקשורת בין חברי הצוות ופנים ארגוניים של הספק) ללא אישור מוקדם לכך מטעם מנהל אבטחת המידע המוסדי.

כל העברת מידע למדיה תקשורתית, חברתית, בכל מדיה שהיא (מודפסת, אלקטרונית, וכו')לרבות פרסומים הנוגעים להתקשרות בעקבות מכרז זה תבוצע אך ורק ע"י דוברות מחב"א ו/או דוברות האוניברסיטה הרלבנטית

ייתכן שבמהלך אירוע או לאחר סיום אירוע הדוברות הרלבנטית תפנה לספק הזוכה ובעיקר לראש צוות המענה בבקשה ל לקבלת מידע על האירוע ולסיוע בהצגת המידע והממצאים. הספק יתמוך בבקשות הדוברות ככל שיעלו.

3.1.12 אישור ביטוח סייבר (S)

על הספק להמציא אישור כי הינו גוף המוגדר ככשיר לפעילות IRT/IR ע"י חברות הביטוח וסוכנויות הביטוח המקובלות בתחום (מארש ישראל סוכנות בטוח בע"מ ודומיה).

בנוסף יידרש הספק לעדכן אישורים אלו מעת לעת בכפוף לשינויים החלים במוסדות.

4. נסיון במגזר האקדמי (בהתייחס למודל "החופש האקדמאי") (S)

החופש האקדמי נועד לאפשר מחקר והוראה בחתירה לאמת המדעית, ללא תלות, ללא מורא וללא משוא פנים. בדיון על חופש אקדמי מקובל להבחין בין חופש המחקר וההוראה לבין חופש פעולה והתבטאות חוץ-אקדמיים. הבחנות אחרות הן בין חופש אקדמי אישי לחופש אקדמי מוסדי ובין ההיבט המנהלי להיבט האקדמאי.

חופש המחקר וההוראה של איש האקדמיה משמעותו הזכות לבחור הן את נושאי המחקר וההוראה והן את אופני המחקר וההוראה, בלי להיות נתון למרות של מקור סמכות, וכל זאת לשם קידומו של הידע האקדמי בצורה המיטבית.

מציע מאשר בזאת כי ידוע ומובן לו שהקשר שבין שירותי IRT/IR לבין חופש האקדמאי יכול להוביל למוסד אקדמאי או חלק ממנו (פקולטה, קבוצת מחקר וכו') לחקור היבטים שונים המחייבים גישה לרשתות תקשורת שונות לרבות אתרים "ברשת האפלה" (קרי Darknet) או למקורות מידע שונים תוך התבססות אפשרית על תשתיות דינמיות בתצורות לא סטנדרטיות. כמו כן החופש האקדמאי יכול לאפשר למנהל המחקר/פקולטה לבחור שלא לאפשר פריסה של חיישני אבטחה מסוימים בתוך תת הרשת שלהם, מה שמחייב "גמישות מחשבתית" וניסיון בהכלת אירועים בסביבה אקדמאית ע"י ספק שירותי ה IRT/IR.

על הספק לפרט את נסיונו במגזר האקדמי תוך התייחסות לנאמר לעיל.

5. מתודולוגיה וחקירת אירועים (S)

חקירת האירוע באתר, איסוף פורנזיקות וניתוח ווקטור פריצה ונוזקות יבוצעו לפי מתודולוגיה סטנדרטיות מומלצות בתחום.

על הספק לפרט את מתודולוגיות ושיטות החקירה המשמשות אותו.

<u>מתודולוגיות לדוגמא:</u>

- SANS Incident Response https://www.sans.org/white-papers/1516/
- NIST SP 800-61r2 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- Mitre Engage https://engage.mitre.org/
- INCD – מתודולוגיית מערך הסייבר (תורת ההגנה בסייבר)

6. צוות IRT – דרישות ומשימות

6.1 צוות IRT (M)

צוות ה Incident Response Team יכלול את כמות האנשים הנדרשים לטיפול באירוע ובכל מקרה לא פחות מ 3 אנשים שיעסקו בטיפול באירוע, בחקירה, בבלימה, בהכלה ובהתאוששות. אחד מהאנשים יהיה ראש הצוות. כמות האנשים בצוות IRT תהיה בסופו של דבר נגזרת של גודל הארגון האקדמאי, כמות ופיזור קמפוסים וחומרת האירוע.

צוותי ה IRT ישתתפו בתהליך ה On-Boarding (התנעת שירות IR/IRT) ויהוו חלק מכל מחזור פעילות ה IR של הארגון בשגרה (התנעה, עדכון תיק אתר, הדרכות, סימולציות וכו') ובחירום.

כמות האנשים בצוות IRT לא תכלול את פונקציות המטה כגון פתיחת אירועים ורישומם, גופי אסקלציית IR בחו"ל או בשותפים, מנהל קשרי לקוח וכו'.

כל חברי צוות ה IRT יצטרכו לחתום על נספח סודיות, נספח קב"ט ולשיקול דעתו של מנהל האבטחה באתר היעד יעברו בדיקת נאותות.

מכיוון שמכרז זה מיועד לשמש מספר גופים אקדמאים, רובם עם מספר קמפוסים ומרכזי מחשוב בפריסה גיאוגרפית רחבה ומכיוון שייתכן מצב בו יותקפו/יפגעו מספר מוסדות אקדמאית במקביל דרישות הקדם במכרז זה לכמות הצוותים והתמהיל שלהם מפורטים להלן:

צוות א' – מורכב מראש צוות, סגן ראש צוות ועוד 3 חברי צוות

צוות ב' – מורכב מראש צוות ו 3 חברי צוות

צוות ג' – מורכב מראש צוות ו 2 חברי צוות

צוות תמיכת תגובה – מורכב מ 3-4 חברי צוות נוספים.

<u>במידה והספק בוחר לחבור לקבלן/ספק משנה ניתן לשלב צוותי תגובה/תמיכה זוטרים בתמהיל זה, יחד עם זאת ראשי צוותים וסגנים יהיו תמיד עובדים של הספק הזוכה.</u>

סה"כ אנשי IRT נדרשים לעמידה מינימלית בדרישות המכרז: 15 אנשי צוות.

דרישות קדם לניסיון, ידע ומיומנות של לחברי צוות השונים מפורט בפרק 3.

צוותי IRT צריכים להגיע עם הציוד המפורט להלן לאירוע בשטח בנוסף לכל ציוד נוסף שמשמש אותם לפעולות אלו:

- מחשבים ניידים לכל חברי הצוות מותקנים עם כלי חקירה, DFIR וכו'
- 4 X דיסקים TB2 חיצוניים חדשים (לצורך פורנזיקה)
- 3 DOK חדשים
- משכפל דיסקים - IDE/SATA NONWRITABLE לשכפול ברמת הבלוק ללא כתיבה למקור.
- ערכת טושים ללוח מחיק
- מטען ובטריית גיבוי לטלפונים ניידים.
- מודם סלולארי USB.
- 5 מגשרי CAT-7E + ג מגשרים אופטיים MM בממשקים שונים.
- חבילת שקיות מסמכים עובי מקסימלי לעדויות DFIR + 25 דפי COC
- שדכן

6.2 עדכון על שינוי ציוות/מצבת כ"א (M)

הספק הזוכה ישלב במענה למכרז קו"ח של כל אנשי התגובה בין אם הם עובדי חברה או עובדי ספק/שותף.

על ספק שזכה ועובד מצוות פעילות שלו מסיים את עבודתו בחברה (בין אם ביוזמת העובד או יוזמת המעביד) לפני טרם תום תקופת ההתקשרות לעדכן על כך, בתוך 10 ימים לכל המאוחר, את מנהל האבטחה בארגון היעד ולהציג בפניו פרטים של עובד אלטרנטיבי בעל אותו ניסיון וכישורים. המוסד האקדמאי שומר לעצמו את הזכות לא לאשר עובד המוצע ולדרוש עובד חלופי.

במידה ועובד של הספק או עובד של ספק משנה באחריותו נמצא מעורב כגורם עוין באירוע סייבר כלשהוא או נמצא מעורב בפלילים, הספק יודיע על כך מיידית למנהל האבטחה בארגון היעד ויפסיק עבודתו במתן השירותים לאלתר.

7. IR Playbook & DFIR (S)

7.1 יצירה/השבחה של נהלי IR ופרוטוקולי תגובה/בלימה

ספק השירות ישלב בתהליך התנעת השירות (On-Boarding) השבחה של נהלי IR ופרוטוקולי תגובה נדרשים להתמודדות עם אירועים שונים. במידה ולארגון האקדמאי יש נהלים קיימים יבוצע השבחה בתיאום ה CISO המקומי, אם לא קיים נוהל יסופק נוהל IR ייעודי לאותו ארגון הנוהל יעבור תהליך אישור ושינויים מול ה CISO בארגון המקומי או גורם מטעמו.

על הספק לפרט את דרכי העבודה שלו בנושא ולספק דוגמא.

7.2 בניית IR Playbook (M)

ספק השירות יכין קובץ IR Playbook שיכלול מענה ל 15 תרחישים/תתי תרחישים שיכללו לכל הפחות את מטריצת האיומים המפורטת בסעיף 7.7 לרבות תתי איומים שונים.

קובץ ה Playbook יבוסס בפועל על 2 קבצים, קובץ תיאור וקובץ תרחיש ואסקלציה.

קובץ תיאור תהליך תגובה יהיה בקובץ WORD/PDF.

קובץ תיאור תרחיש יהיה בפורמט VISIO.

תיאור תכולת הקבצים:

קובץ תיאור מבוסס MS WORD/PDF שיכלול:

- רשימת בעלי תפקידים
- אסקלציות לפי חומרה/זמן
- תיאור סוג האירוע
- דרכי יצירת קשר

עדכון IR Playbook

הספק יעדכן את ה IR Playbook אחת לרבעון ובהלימה לשינויים מבניים/תהליכיים שבוצעו בארגון היעד. כמו כן הספק יפרט מתי בוצעו העדכונים האחרונים למסמך ה Playbook הראשוני שהוא מביא איתו לתהליך ההתנעה.

7.3 תיאור ותיוג אירועים ואיומים בפועל (S)

הספק יפרט איך הוא מנהל תיוג ורישום אירועים לרבות דוגמא לטופס תיוג, רישום דיגיטלי במערכת Trouble Ticket ו/או רישום ידני

7.4 פרוטוקולים להכלה ובלימת אירוע (S)

הספק יפרט דוגמא לפרוטוקולים להכלה ובלימת אירוע לרבות דוגמאות לאכיפת מדיניות וכלים, התבססות על טכנולוגיות קיימות במוסד האקדמאי או על ציוד נפרס כחלק מהשירות וכו'

7.5 קובץ תרחישים ואסקלציה מבוסס MS Visio (S)

יצירת ה IR Playbook תכלול חוברת תרחישים שתוגש בפורמט VISIO ותכלול לכל הפחות את האלמנטים הבאים:

- תרשים אסקלציה והפעלת IR משלב הזיהוי ועד סיום האירוע
- הוספת בעלי תפקידים לתרחיש
- הוספת פרקי זמן לאסקלציה

על הספק לצרף דוגמא לתרחיש אחד לפחות.

7.6 מטריצת איומים מינימלית (S):

על הספק לפרט את דרכי הפעולה במענה למטריצת האיומים כך שתכלול לפחות את האיומים הבאים:

א. Malware - "קוד עוין/זדוני" לא ממוקד

ב. חדירה רשתית- Network Intrusion

ג. זליגת מידע Data Leakage/Data Loss

ד. התקפת מניעת שרות/DOS רשתי

ה. התקפת מניעת שרות/DOS אפליקטיבי

ו. התקפת מניעת שרות/DDOS רשתי

ז. התקפת מניעת שרות/DDOS אפליקטיבי

ח. קוד עוין מסוג Ransomware/Cryptoware – "תוכנת כופר/סוחטה"

ט. קוד עוין מסוג "Wiper" או דומה

י. איום השחתה וונדליזם - Defacing

יא. XSS (Cross-Site Scripting), OWASP Top 10 Attacks, WHP ("Water Hole Poisoning)

7.7 תיעוד אירוע ותהליכים (M):

הספק יצור את הקבצים הבאים כחלק מתהליך ניהול האירוע:

א. קובץ ניהול אירועים:

קובץ EE&ML – Events Escalation & Management Log משמש כמנגנון לרישום ותיעוד יומן התגובה והפעלת נהלי התאוששות מאירועי סייבר מורכבים. הקובץ מאפשר לבנות כלי לתחקור נהלי התגובה ומעקב מרגע זיהוי האיום ועד להתאוששות מלאה.

ניתן להזין את המידע לכל בסיס נתונים מבני, לרבות שימוש בקבצי אקסל, יישומי ACCESS, ODBC וכו'.

מידע שנדרש לכלול בקובץ:

- מספר ומק"ט אירוע
- תיעוד כרונולוגי של כל התהליכים ובעלי התפקיד מרגע זיהוי אירוע
- תיאור אירוע
- וקטור תוקף/"קורבן"
- ממצאים
- לכל שלב – משתתפים, החלטות, הסתייגויות.
- לוח זמנים לכל תת-שלב בתהליכי הבלימה והתאוששות
- הפתרון שיושם
- נהלים/חריגה מנהלים
- קבוצות משולבות
- משאבים בשימוש (תיעוד חמ"ל וכו')
- HASH ומזהים שנאספו במהלך החקירה
- ספריות פורנזיקה
- עדויות
- צילומי מסך

- תיעוד הכלים ששימשו לחקירת האירוע
- סוג מידע שנפגע/זלג.
- עותק טופס COC

ב. קובץ תיוג, תיעוד וחקירת אירוע :

תיוג ותיעוד האירוע הוא תהליך חובה ויפעל כרכיב תיעוד מרכזי לכל סוגי האירועים. המידע בין אם ישמר בקובץ או באפליקציה ישמש לאיסוף מודיעין פורנזיקות הקשורות לאירועים חיצוניים ופנימיים וכן מאפשר בניית כלי לשימור ידע ותחקור אירועים. המידע יוכל לשמש בעתיד לפלטפורמות היזון מודיעין וניהול אירועים. ניתן להזין את המידע לכל בסיס נתונים מבני, לרבות שימוש בקבצי אקסל, יישומי ACCESS, ODBC וכו'.

מידע שנדרש לכלול בקובץ:

- Time Stamp + Intervals
- Event Number = Mapped to EE&ML File
- PZ Information (IP, Hostname, Username, Domain, etc)
- PZ Neighbors with IOC
- Target Category – Host, Server (BM/VM), Network Device.
- Threat Vector – Attacker ID, SRC/DST/ C&C, Ingress/Egress Traffic
- Known Vulnerability at Target
- Exploit Used
- AS – Attack Surface – WEB/MAIL/MIME/FTP/Human/Network
- Authentication Level Breached
- Root Cause Analysis
- Single Step Attack/ Multi Phase/Step-phase Attack
- Payload
- Severity
- Mobility
- Action + Time Stamp

7.8 הפעלת נוהל DFIR לשמירת רצף עדויות ושימור מידע פורנזי (S):

עבור חלק מהאירועים נדרש לשמר ראיות פורנזיות למטרות שונות.

הספק נדרש לפרט את התייחסותו להפעלת נוהל DFIR על בסיס המפורט להלן:

איסוף המידע יבוצע במודל COC – Forensics Chain of Custody.

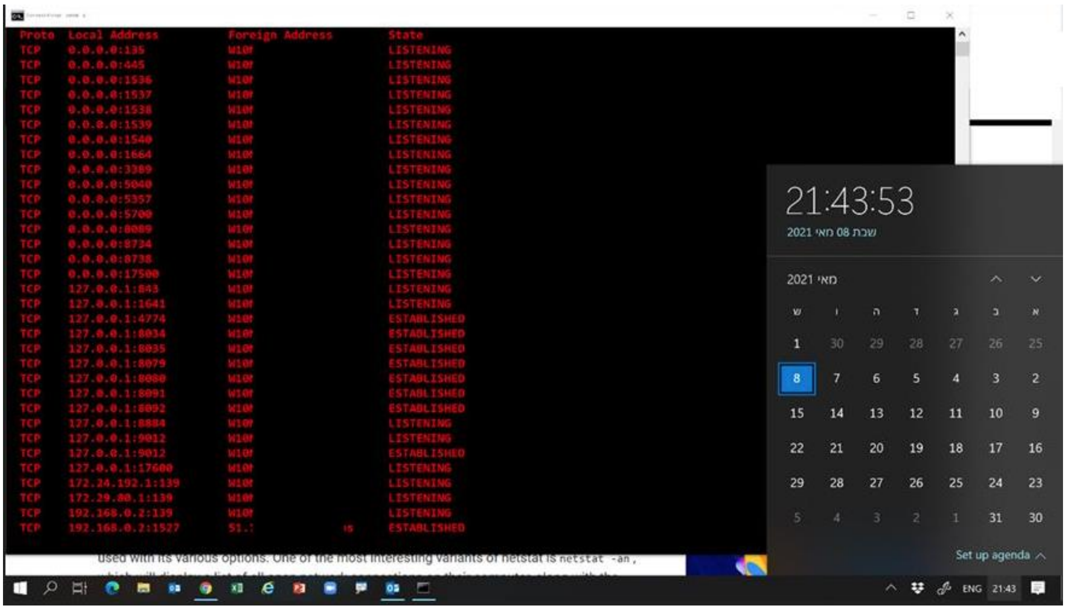
החלטה על הפעלת נוהל COC תבוצע ע"פ המלצת נותן השירות ו/או הנחיה של מנהל אבטחת מידע במוסד האקדמאי.

מכיוון שחלק מהאירועים הנחקרים קשורים לאיומים בעלי יכול "ניוד/ניידות" גבוהה (Lateral Movement) יש חשיבות לניתוק התחנה/מקור האיום מהרשת בהקדם האפשרי אך לא לפני שמבוצע מיפוי רשתי בזמן אמת – זהו מידע פורנזי קריטי שלא ניתן לבצע לאחר ניתוק

התחנה/השרת מהרשת ועלול להוביל לאובדן ראיות הקשורות לגורם עוין חיצוני. לכן את תהליך איסוף המידע בשלבים הבאים יש לבצע לפני הפעלת נוהל בלימה.

כל איסוף המידע בתחנת מקור האיום הנחקר ו/או בתחנת PZ יבוצע לספרייה במחיצה הראשית שתתבסס על סכמת שם המכילה תאריך, קוד אירוע ושם האנליסט החוקר ברשת תיבות לדוגמא: C:\Malware200901_070521_TN\.

בנוסף לשמירת פלט הבדיקות יבוצע צילום מסך שיכלול תמונה של הטבעת תאריך ושעה ושם המחשב. לדוגמא:



התמונות ישמרו באותה מחיצה, עותק מהתמונות יועבר ל DOK ייעודי שיעבור הלבנה וסריקה של מספר מערכות כהכנה להמשך חקירה.

תחילת חקירה

צוות התגובה יבצע מספר פקודות ותהליכים, פקודות אלו יבוצעו ב Command Prompt עם ההרשאות המינימליות הנדרשות, כאמור הפלט יכוון לספריית הראיות, לדוגמא: C:\Malware200901_070521_TN\.

<u>איסוף מידע לפני ביצוע Quarantine וניתוק מהרשת – רשימה חלקית, על המציע לפרט שלל בדיקות ואיסוף מידע:</u>

- Ipconfig /all >> C:\Malware200901_070521_TN\net1.txt
- Tracert 194.90.1.5 >> C:\Malware200901_070521_TN\net2.txt
- Netstat –an >> C:\Malware200901_070521_TN\net3.txt
- Nslookup www.XXX.com >> C:\Malware200901_070521_TN\net2.txt
- Net share >> C:\Malware200901_070521_TN\net1.txt

- Tasklist /svc >> C:\Malware200901_070521_TN\tasklist.txt

<u>איסוף מידע לאחר ביצוע Quarantine ולאחר ניתוק מהרשת- רשימה חלקית, על המציע לפרט שלל בדיקות ואיסוף מידע :</u>

- Task list >> C:\Malware200901_070521_TN\epstat_1.txt
- Reg Query HKLM\software\ >> C:\Malware200901_070521_TN\epstat_2.txt
- Netsh firewall show state >> C:\Malware200901_070521_TN\firewall.txt
- Net user >> C:\Malware200901_070521_TN\netuser.txt
- Net accounts >> C:\Malware200901_070521_TN\netaccounts.txt
- Reg Query HKLM\software\Microsoft >>
- C:\Malware200901_070521_TN\epstat_2.txt
- Systeminfo >> C:\Malware200901_070521_TN\sysinfo.txt
- Eventvwr.msc
- RESMON + Printscr
- אם מדובר בתחנת/שרת LINUX יש לצרף פלט פורנזי ממערכות כגון GRR, MEMmap Linux FTK, וכו'

<u>יצירת עותק קוהרנטי של הדיסק</u>

מדובר בשלב קריטי בנוהל ובשימור הראיות, בשלב זה אנליסט שמטפל בחקירה יבצע העתק 1:1 של הדיסק המקורי ברמת הבלוק (כולל הספרייה החדשה שנוצרה ומכילה את הראיות) את הגיבוי יש לסיים ביצירת תת ספריית HASH של הכונן כולו וכן של ספריות שחשודות לחקירה. משלב זה ואילך כל הבדיקות יבוצעו על העותק הגיבוי בלבד והדיסק המקורי יישמר תחת תת-נוהל ICOC – שמירת רצף עדויות (מפורט בהמשך).

<u>שמירת Meta Data אנליטי – חקירת תחנת קצה</u>

באחריות אנליסט שעוסק בחקירה להקים קובץ תיוג וקובץ לוג חקירה (תוכן מפורט בהמשך) תחת ספריית חקירה ייעודית שתוקם ברשת.

<u>חקירות רוחב –איומי תחנות קצה/שרתים</u>

באחריות אנליסט שעוסק בחקירה לבצע חקירות רוחב במידה ויש חשש לזיהוי IOC בתחנות/שרתים נוספים/ות או לאירוע הקשור לקוד עוין בעל יכולת ניוד מתקדמת.

בנוסף למפורט לעיל על איסוף פורנזיקות, על הספק לפרט את שלל הכלים שבשימושו שישולבו בתהליך החקירה ובתהליך איסוף ושמירת העדויות הפורנזיות במהלך אירוע.

7.9 איסוף וגיבוי עדויות פורנזיות (M):

הספק מתחייב לבצע איסוף וגיבוי עדויות פורנזיות תוך שמירה על רצף ראיות (COC) ועמידה בדרישות המפורטות להלן (לאחר יצירת עותק והעברתו לחוקר הסייבר הרלוונטי):

- מחשב נייח – יבוצע פירוק של הדיסק/ים, הכנסה לשקית מסמכים/מעטפת עדויות חתימה עם טופס COC, שידוך והעברה לכספת.

- מחשב נייד/טאבלט – במידת האפשר פירוק הדיסק והמשך כמו בתהליך של מחשב נייח, אחרת הכנסת כל המחשב לשקית חתומה או חתימת המחשב עצמו עם שרוול למניעת פתיחה (דוגמאות בהמשך).
- DOK/דיסק חיצוני/נייד – בדומה לטיפול בדיסק של מחשב נייח.
- שרת – בהלימה לנהלי בלימה, גיבוי והתאוששות, הסרת הדיסק, התקנת דיסק חדש עם גיבוי, סריקה, המשך טיפול כמו במחשב נייח.
- טלפון נייד – תלוי תצורה, וקטור/איום – ייקבע נקודתית ע״י מנהל אבטחה
- טלפון IP - הסרה, תיוג והחתמה.

<u>טופס Chain of Custody לדוגמא</u>

<u>דוגמא 1:</u>

תאריך תיוג/נעילה	אנליסט/חוקר אירוע	מנהל אירוע בכיר	קוד אירוע/תג אירוע	תיאור מקור מידע
HASH	**ספריית פורנזיקה קשורה**	**לוג חקירה**	**פרטים נוספים**	

מידע נוסף:

שם וחתימת חוקר סייבר

שם וחתימת מנהל אירוע בכיר

דוגמא 2:

Print Form

PROPERTY / EVIDENCE CHAIN OF CUSTODY FORM

APLCS, LLC (http://www.aplcs.com)

Case Name:		**Reason Obtained:**	
Case Number:			
Item Number:	**Evidence Type / Manufacturer:**	**Model Number:**	**Serial Number:**
Content Owner / Title:	**Content Description:**		
Content Owner Contact Information:			
Forensic Agent:	**Creation Method:**	**HASH Value:**	**Creation Date/Time:**
Forensic Agent Contact Information:			

CHAIN OF CUSTODY

Tracking Number	Date / Time	Released By	Received By	Reason for Change
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	

Item Number: ______________________

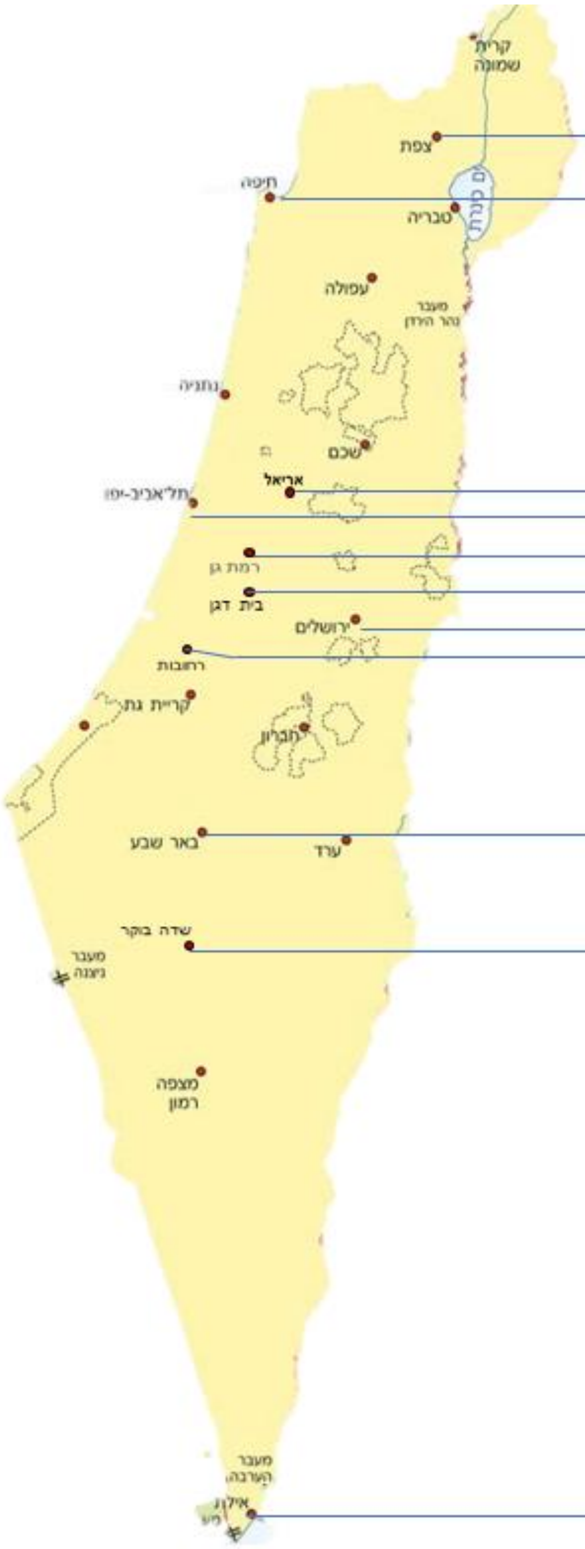
Page: 1 of ______

8. מוסדות אקדמאיים ופריסה גיאוגרפית

8.1 רשימת המוסדות האקדמאיים הרלוונטיים (I)

מוסד אקדמאי	קמפוס
אוניברסיטת בן גוריון	קמפוס מרקוס
	שדה בוקר
	אילת
	בית היאס
	קריית ברגמן
אוניברסיטת בר אילן	קמפוס רמת גן
	הפקולטה לרפואה
אוניברסיטת חיפה	קמפוס ראשי
האוניברסיטה העברית	הר הצופים
	גבעת רם
	עין כרם
	חקלאות
	אילת
	בית חולים וטרינרי
האוניברסיטה הפתוחה	רעננה
	רמת אביב
	ירושלים
	חיפה
הטכניון	הטכניון קמפוס ראשי
	הטכניון בית ספר לרפואה
	הטכניון שרונה
מכון ויצמן	קמפוס ראשי
אוניברסיטת תל אביב	קמפוס ראשי
אוניברסיטת אריאל	קמפוס ראשי

8.2 פיזור גיאוגרפי של קמפוסים (I)



הגדרת אזור	עיר/ישוב
EX1	צפת
NA1	חיפה
CA1	אריאל
CA1	תל-אביב
CA1	רמת גן
CA1	בית דגן
CA2	ירושלים
CA1	רחובות
SA1	באר שבע
EX1	שדה בוקר
EX2	אילת

9. תכולת שירותים אופציונליים (G)

הספק מוזמן להציע מכלול של שירותים נוספים המוגדרים "כהרחבות אופציונליות" על בסיס ניסיונו ויכולתו או על בסיס שיתוף פעולה עם גוף מוביל בתחום. יש להרחיב על כל שירות אופציונלי בנספח שיצורף למענה. מובהר בזאת כי הרחבות אופציונליות כאמור לא יזכו בשקלול בנקודות נוספות.

ראה נספח 12

מס'	שירות אופציונלי/הרחבת שירות	דרישות קדם מינימליות
1	הדרכות סייבר ומענה לאיומים	ביצוע הדרכות ב 5 לקוחות לפחות בשנתיים האחרונות יש לצרף תקציר הדרכה לדוגמא שבוצעה עבור לקוח בשנתיים האחרונות יש לצרף את רשימת הלקוחות והמלצה משני לקוחות בשנתיים האחרונות
2	כתיבת נוהל מענה "לאירוע משבר סייבר"	כתיבת נהלים משמעותיים להנהלה – לפחות 5 לקוחות בשנתיים האחרונות יש לצרף את רשימת הלקוחות והמלצה משני לקוחות בשנתיים האחרונות
3	ביצוע תרגילי סימולציה אירוע סייבר – Red/Blue Team לאנשי אבטחת מידע	ביצוע לפחות 8 תרגילים בשנה האחרונה
4	תרגילי סימולציה אירוע סייבר משולב הנהלה	ביצוע לפחות 3 תרגילים משולבי הנהלה בכירה בשנה האחרונה
5	ניהול מו"מ תוקפים : • תקשורת עם גוף תוקף • ניהול אירוע מורכב • ניתוח מוטיבציית תוקף – תודעה/כספי/וכו' • ייעוץ לרובד הנהלה • ניתוח מודיעין • סיוע בנושא תשלומים • התנהלות אל מול המבטח	ביצוע מו"מ עד לסיום אירוע – לפחות 3 אירועים בשנתיים האחרונות ניסיון מוכח בבחינת קשרי גופי טרור לאמצעי התשלום לרבות גישה וניסיון באיתור קשרי טרור לארנקי מטבעות דיגיטליים. לפחות 3 שנות נסיון בניהול משברים ומו"מ לפחות 5 חברי צוות מומחים בניהול מו"מ נסיון מוכח עם לפחות שתי חברות ביטוח של המוסדות. יש להעביר לפחות 3 ממליצים רלוונטיים מגופים מובילים במשק.
6	שירות אסקלציית IR בינלאומית	שיתוף פעולה עם גוף אסקלציית IR בינלאומי מוכר שמטפל במאות אירועים בלקוחות גדולים

10. היפרדות

התנאים והמועדים שבהם תהיה מחב"א ו/או יהיה מוסד רשאים להפסיק ההתקשרות עם הספק הזוכה, מבלי שיהיה עליהם לשלם לו כל פיצוי, או כנגד קבלת פיצוי מהספק בגין הפרותיו, מפורטים בהסכם המצורף למכרז זה ומהווה חלק בלתי נפרד ממנו.

הספק מתחייב להסיר ממערכות המוסד כל כלי תוכנה שהותקן במהלך השירות לצורך ובמהלך הפעילות

11. עלות

11.0 כללי

א. המענה הכספי למכרז יעשה על גבי נספח 11 "מענה כספי" והוא יכלול את טבלאות פרק העלות.

11.0.1 אופן התשלום

א. כל המחירים שיהיו נקובים בהצעה יהיו סופיים, ויכללו את כל מרכיבי העלות, מיסים (למעט מע"מ), היטלים או תוספות אחרות, לרבות כל תשלום מסוג כלשהו לצד שלישי בגין תמלוגים ו/או זכויות שימוש.

ב. המחירים יהיו נקובים בשקלים,

ג. המחירים יוצמדו למדד אחת לשנה ויעודכנו בעת שהמדד יעלה בשיעור של מעל 4% לעומת המדד שיהיה ידוע בעת מתן הודעה על הזכיה.

ד. התשלום לספק יעשה אחת לרבעון , וישולם על בסיס שוטף + 60 ימים.

נספח 1.3.3 גלופה להעברת שאלות ובקשות הבהרה

יצורף קובץ אקסל כנספח 1.3.3

נספח 1.6.2 מעמדו המשפטי של המציע

א. צורת ההתאגדות של המציע (חברה / עמותה / שותפות / אחר) ____________________

ב. מספר מזהה (לפי הרישום במרשם הרלוונטי) ____________________________

ג. המדינה בה התאגד המציע ______________________

ד. מורשי החתימה בשם המציע ותפקידם אצל המציע:

#	שם	ת.ז.	תפקיד בתאגיד	דוגמת חתימה

ה. צירוף מסמכים נדרשים (סמן ☑ במקום המיועד לכך אם צורך):

המסמך הנדרש	האם צורך? (סמן ☑)
אישור על רישום התאגיד	❐
נסח רישום תאגיד עדכני לשנת 2023	❐
אישור של עו"ד בדבר זהות מורשי החתימה אצל המציע	❐

אישור עורך הדין

אני החי"מ, עו"ד______________________, מרח' ________________________, מאשר בזה כי המציע המפורט לעיל קיים, פרטיו המצוינים לעיל נכונים והמורשים לחתום בשמו ולחייבו בחתימתם הם אלה הרשומים בפיסקה ד' דלעיל.

תאריך	מספר רישיון	חתימה וחותמת
___________________	_____________________	_____________________

נספח 1.6.3 - עמידה בהוראות חוק עסקאות גופים ציבוריים ושמירה על דיני עבודה

א. צירוף מסמכים נדרשים

סמן ☑ במקום המיועד לכך אם צורך:

המסמך הנדרש	האם צורף? (סמן ☑)
אישור תקף על ניהול פנקסי חשבונות ורשומות לפי חוק עסקאות גופים ציבוריים	❒

ב. תצהיר מאומת ע"י עו"ד בדבר היעדר הרשעות בעבירות לפי חוק עובדים זרים

אני הח"מ ______________ ת.ז. ______________ לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

הנני נותן תצהיר זה בשם ____________________ שהוא המציע (להלן: "**המציע**") המבקש להתקשר עם עורך ה**מכרז הפומבי מספר 2-2023 שירותי IR\IRT למחב"א והמוסדות האקדמאים החברים בה**.
אני מצהיר/ה כי הנני מוסמך/ת לתת תצהיר זה בשם המציע.

בתצהירי זה, משמעותו של המונח "**בעל זיקה**" כהגדרתו בחוק עסקאות גופים ציבוריים התשל"ו-1976 (להלן: "**חוק עסקאות גופים ציבוריים**"). אני מאשר/ת כי הוסברה לי משמעותו של מונח זה וכי אני מבין/ה אותו.

משמעותו של המונח "**עבירה**" – עבירה לפי חוק עובדים זרים (איסור העסקה שלא כדין והבטחת תנאים הוגנים), התשנ"א-1991 או לפי חוק שכר מינימום התשמ"ז-1987, ולעניין עסקאות לקבלת שירות כהגדרתו בסעיף 2 לחוק להגברת האכיפה של דיני העבודה, התשע"ב-2011, גם עבירה על הוראות החיקוקים המנויות בתוספת השלישית לאותו חוק.

המציע הינו תאגיד הרשום בישראל.

(סמן ☑ במשבצת המתאימה)

❒ המציע ובעל זיקה אליו <u>**לא הורשעו**</u> ביותר משתי עבירות עד למועד האחרון להגשת ההצעות (להלן: "**מועד להגשה**") במכרז פומבי מספר 2-2023 שירותי IR\IRT למחב"א והמוסדות האקדמאים החברים בה.

❒ המציע או בעל זיקה אליו <u>**הורשעו**</u> בפסק דין ביותר משתי עבירות <u>**וחלפה שנה אחת**</u> לפחות ממועד ההרשעה האחרונה ועד למועד ההגשה.

❒ המציע או בעל זיקה אליו <u>**הורשעו**</u> בפסק דין ביותר משתי עבירות <u>**ולא חלפה שנה אחת**</u> לפחות ממועד ההרשעה האחרונה ועד למועד ההגשה.

זה שמי, להלן חתימתי ותוכן תצהירי דלעיל אמת.

______________	______________	______________
תאריך	שם	חתימה וחותמת

אישור עורך הדין

אני הח"מ ______________________, עו"ד מאשר/ת כי ביום _____________ הופיע/ה בפני במשרדי אשר ברחוב _____________ בישוב/עיר _____________ מר/גב' _______________ שזיהה/תה עצמו/ה על ידי ת.ז. _____________ /המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, אישר את אמיתות האמור בתצהיר זה חתם/ה עליו בפני .

____________________	____________________	____________________
תאריך	מספר רישיון	חתימה וחותמת

נספח 1.6.4 – תצהיר בדבר ניסיון המציע

לכבוד: מחב״א

הנדון: **מכרז פומבי מספר 2-2023 שירותי IR\IRT למחב״א והמוסדות האקדמאים החברים בה להלן - ״המכרז״)**

1. אני הח״מ, **מורשה החתימה** והמוסמך לתת תצהיר בשמה של חברת _______________, המציעה במכרז (להלן – ״המציע״):

שם מורשה החתימה	ת.ז	חותמת תאגיד	חתימה אישית	תאריך

2. לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר כדלקמן:

א. המציע הינו ארגון שירותי IR/IRT עם ניסיון מוכח במתן שירותי IR/IRT לארגונים גדולים וניסיון מוכח בניהול, הכלה והתאוששות מאירועי סייבר מורכבים (יש לפרט בנספח לתצהיר היסטוריית אירועים גם מבלי לחשוף שם לקוח).

ב. למציע ישנם מספר לקוחות פעילים בשירות IRT/IR: 10 (יש לצרף בנספח לתצהיר רשימת לקוחות ורשימת אנשי קשר).

ג. למציע יש ניסיון מוכח בניהול אירוע סייבר משמעותי: 12 אירועים בשנתיים האחרונות, מתוכם לפחות 2 אירועי סחיטה/כופרה (יש לפרט בנספח לתצהיר רשימת אירועים, ניתן לצרף טופס סודיות כשלב מקדים).

ד. למציע יש ניסיון מוכח בכתיבת IR Playbook עם לפחות 15 תרחישים ב **6** לקוחות שונים. יש לספק בנספח לתצהיר דוגמא מושחרת, רשימת לקוחות ואנשי קשר.

ה. למציע יש צוות מקצועי בהתאם למפורט בסעיף 1.6.4.2 למכרז.

ו. המציע יכול לספק SLA בפיזור גיאוגרפי בהתאם למפורט בסעיף 1.6.4.4 למכרז.

זה שמי, להלן חתימתי ותוכן תצהירי דלעיל אמת.

____________________	____________________	____________________
תאריך	שם	חתימה וחותמת

אישור עורך הדין

אני הח״מ ____________________, עו״ד מאשר/ת כי ביום ______________ הופיע/ה בפני במשרדי אשר ברחוב ______________ בישוב/עיר ______________ מר/גב' ________________ שזיהה/תה עצמו/ה על ידי ת.ז. ______________/ המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

____________________	____________________	____________________
תאריך	חותמת ומספר רישיון	חתימה

נספח 1.6.5 תצהיר בדבר היעדר ניגוד עניינים

שנערך ונחתם ב__________ ביום _____ בחודש ______ שנת________

אני_____________ הח״מ, נושא ת.ז. ____________ נותן תצהירי זה בקשר **מכרז פומבי מספר 2-2023 שירותי IR\IRT למחב״א והמוסדות האקדמאים החברים בה**.

הנני נותן תצהירי זה בשם תאגיד _____________________, שמספרו המזהה הוא _________________ (להלן – המציע).

הנני מכהן במציע בתפקיד _____________________.

הנני מורשה חתימה במציע ויש בחתימתי כדי לחייב את המציע.

הואיל ומחב״א והמוסדות החברים בה עשויים לקבל את השירותים/הטובין כהגדרתם להלן;

והואיל והנני עשוי להיות מועסק על ידי המציע בקשר למתן השירותים/הספקת הטובין;

והואיל והנני עשוי להימצא במצב של ניגוד עניינים במסגרת מתן השירותים ולאחריו;

לפיכך הנני מצהיר ומתחייב כלפי מחב״א והמוסדות כדלקמן:

א. הגדרות

בהתחייבות זו תהיה למונחים הבאים המשמעות המופיעה לצידם:

״השירותים/ - שרותי IR/IRT

״עובד״ - כל אחד מעובדי המציע אשר באמצעותו יינתנו השירותים למזמין.

ב. הנני מצהיר כי למיטב ידיעתי אין לי, למציע ו/או מי מעובדיו ולא יהיה לי ולהם, במהלך תקופת מתן השירותים, ובמהלך שלושה חודשים מתום תקופה זו, ניגוד עניינים מכל מין וסוג שהוא בין מתן השירותים נשוא המכרז לבין קשרים עם גורמים בעלי עניין בתחום האמור, למעט באם ועדת המכרזים אישרה בכתב, לאחר שהעובדות הוצגו בפניה, כי אין בעובדות שאציג בפניה משום ניגוד עניינים או באם קיים ניגוד עניינים מדובר בניגוד עניינים שולי אשר אין בו השפעה על השירותים נשוא המכרז.

ג. הנני מצהיר ומתחייב כי בתקופת מתן השירותים ושלושה חודשים אחריה, אני, המציע ועובדיו שלא ניתן את השירותים לכל גורם שהוא אם מתן השירותים לגורם כאמור תסתור את פעילותנו למען המזמין אלא אם כן התקבל לכך אישור מראש ובכתב של המזמין.

ד. הנני מתחייב להודיע למזמין באופן מידי על כל נתון או מצב, שבשלם אני המציע ו/או מי מעובדיו עלול להימצא במצב של ניגוד עניינים, מיד עם היוודע לי הנתון או המצב האמורים.

ה. הנני מצהיר ומתחייב לדווח מראש למזמין על כל כוונה של המציע, להתקשר עם כל גורם כאמור בסעיפים ב-ג לעיל, בניגוד להתחייבויותיי בסעיפים אלו, ולפעול בהתאם להוראותיו בעניין. המזמין רשאי לא לאשר לי התקשרות כאמור או לתת הוראות אחרות שיבטיחו העדר ניגוד עניינים, והנני מתחייב כי אפעל בהתאם להוראות אלו, בהקשר זה.

זה שמי, להלן חתימתי ותוכן תצהירי דלעיל אמת.

________________	________________	________________
תאריך	שם	חתימה וחותמת

אישור עורך הדין

אני החי"מ ______________________, עו"ד מאשר/ת כי ביום _____________ הופיע/ה בפני במשרדי אשר ברחוב _____________ בישוב/עיר _____________ מר/גב' _______________ שזיהה/תה עצמו/ה על ידי ת.ז. _____________ /המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

____________________	____________________	____________________
תאריך	חותמת ומספר רישיון	חתימה

נספח 1.6.6 תצהיר כללי

א. פרטי המציע

אני_______________ הח״מ, נושא ת.ז. _____________ נותן תצהירי זה בקשר **מכרז פומבי מספר 2-2023 שירותי IR\IRT למחב״א והמוסדות האקדמאים החברים בה**.

הנני נותן תצהירי זה בשם תאגיד ______________________, שמספרו המזהה הוא _______________ (להלן – המציע). התאגיד התאגד ב_________________.

הנני מכהן במציע בתפקיד ______________________.

הנני מורשה חתימה במציע ויש בחתימתי כדי לחייב את המציע.

במציע קיימים מורשי חתימה נוספים שהם (שם, ת.ז.):

1. ______________________________________.
2. ______________________________________.
3. ______________________________________.

ב. הסכמה לדרישות המכרז

קראתי את כל תנאי **מכרז פומבי מספר 2-2023 שירותי IR\IRT למחב״א והמוסדות האקדמאים החברים בה** ודרישותיו, הבנתי אותם ואני מתחייב בשם המציע ומטעמו כי המציע ימלא אחר כל התנאים והדרישות של המכרז, ההצעה וההסכם, בדייקנות, ביעילות, במומחיות ובמיומנות, לשביעות רצון עורך המכרז, ובמועדים אשר ייקבעו על ידו, והכל בכפוף להוראות מכרז זה וההסכם.

הנני מצהיר כי כל הנתונים המפורטים בהצעה למכרז נבדקו על ידי והם נכונים ומדויקים.

ג. הצהרה על שימוש בתוכנות מקוריות וזכויות קניין

הנני מצהיר כי המציע משתמש בתוכנות מחשב מקוריות בלבד.

הנני מצהיר כי המציע הוא בעל זכויות הקניין, זכויות הפטנטים, זכויות היוצרים והזכויות האחרות הגלומות בהצעתו (להלן ביחד - ״זכויות הקניין״) או שהמציע מורשה לעשות שימוש בזכויות הנ״ל, ולא קיימת מניעה משפטית כל שהיא להגיש הצעתו ולהתקשר לפיה עם עורך המכרז כמפורט במכרז.

המציע מתחייב לשפות ולפצות את עורך המכרז בגין נזקים כלשהם בשל תביעות צד ג' נגדו כתוצאה מהפרת זכויות קניין כלשהן בשל ההצעה או ההתקשרות של עורך המכרז.

ד. הצהרה בדבר אי תיאום הצעות במכרז

המחירים אשר מופיעים בהצעה זו נקבעו על ידי התאגיד באופן עצמאי, ללא התייעצות, הסדר או קשר עם מציע אחר או עם מציע פוטנציאלי אחר (למעט קבלני המשנה אשר צוינו בהצעה).

המחירים המופיעים בהצעה זו לא הוצגו בפני כל אדם או תאגיד אשר מציע הצעות במכרז זה או תאגיד אשר יש לו את הפוטנציאל להציע הצעות במכרז זה.

לא הייתי מעורב בניסיון להניא מתחרה אחר מלהגיש הצעות במכרז זה.

לא הייתי מעורב בניסיון לגרום למתחרה אחר להגיש הצעה גבוהה או נמוכה יותר מהצעתי זו.

לא הייתי מעורב בניסיון לגרום למתחרה להגיש הצעה בלתי תחרותית מכל סוג שהוא.

הצעה זו של התאגיד מוגשת בתום לב ולא נעשית בעקבות הסדר או דין ודברים עם מתחרה או מתחרה פוטנציאלי אחר במכרז זה.

יש לסמן ☑ במקום המתאים

❒ למיטב ידיעתי, התאגיד מציע ההצעה לא נמצא כרגע תחת חקירה בחשד לתיאום מכרז

אם כן, אנא פרט:

____
____
____

אני מודע לכך כי העונש על תיאום מכרז יכול להגיע עד חמש שנות מאסר בפועל לפי סעיף 47א לחוק ההגבלים העסקיים, תשמ״ח-1988.

זה שמי, להלן חתימתי ותוכן תצהירי דלעיל אמת.

______________	______________	______________
תאריך	שם	חתימה וחותמת

אישור עורך הדין

אני החי״מ ______________, עו״ד מאשר/ת כי ביום ________ הופיע/ה בפני במשרדי אשר ברחוב ________ בישוב/עיר ________ מר/גב' ________ שזיההה/תה עצמו/ה על ידי ת.ז. ________ /המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

______________	______________	______________
תאריך	חותמת ומספר רישיון	חתימה

נספח 1.6.7 - תצהיר בדבר העסקת אנשים עם מוגבלות

אני הח"מ _______________ ת.ז. _______________ לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

הנני נותן תצהיר זה בשם ___________________ שהוא המציע (להלן: "**המציע**") המבקש להתקשר עם עורך **מכרז פומבי מספר 2-2023 שירותי IR\IRT למחב"א והמוסדות האקדמאים החברים בה**. אני מצהיר/ה כי הנני מוסמך/ת לתת תצהיר זה בשם המציע.

(סמן ☑ במשבצת המתאימה):

❒ הוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח 1998 לא חלות על המציע.

❒ הוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח 1998 חלות על המציע והוא מקיים אותן.

(במקרה שהוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח 1998 **חלות על המציע** נדרש לסמן x במשבצת המתאימה):

❒ המציע מעסיק פחות מ-100 עובדים.

❒ המציע מעסיק 100 עובדים או יותר.

(במקרה שהמציע מעסיק 100 עובדים או יותר נדרש לסמן X במשבצת המתאימה):

❒ המציע מתחייב כי ככל שיזכה במכרז יפנה למנהל הכללי של משרד העבודה והרווחה והשירותים החברתיים לשם בחינת יישום חובותיו לפי סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח 1998, ובמקרה הצורך – לשם קבלת הנחיות בקשר ליישומן.

❒ המציע התחייב בעבר לפנות למנהל הכללי של משרד העבודה והרווחה והשירותים החברתיים לשם בחינת יישום חובותיו לפי סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח 1998, הוא פנה כאמור ואם קיבל הנחיות ליישום חובותיו **פעל ליישומן** (במקרה שהמציע התחייב בעבר לבצע פנייה זו ונעשתה עמו התקשרות שלגביה נתן התחייבות זו).

המציע מתחייב להעביר העתק מהתצהיר שמסר לפי פסקה זו למנהל הכללי של משרד העבודה הרווחה והשירותים החברתיים, בתוך 30 ימים ממועד ההתקשרות.

זה שמי, להלן חתימתי ותוכן תצהירי דלעיל אמת.

תאריך	שם	חתימה וחותמת
___________________	___________________	___________________

אישור עורך הדין

אני הח"מ ____________________, עו"ד מאשר/ת כי ביום ______________ הופיע/ה בפני במשרדי אשר ברחוב ______________ בישוב/עיר ______________ מר/גב' ______________ שזיהה/תה עצמו/ה על ידי ת.ז. ______________/המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

תאריך	חותמת ומספר רישיון	חתימה
___________________	___________________	___________________

נספח 1.6.8 תצהיר בדבר זמינות מיידית

אני הח"מ ________________ ת.ז. ________________ לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

הנני נותן תצהיר זה בשם ____________________ שהוא המציע (להלן: "**המציע**") המבקש להתקשר עם עורך **מכרז פומבי מספר 2023-2 שירותי IR\IRT למחב"א והמוסדות האקדמאים החברים בה**. אני מצהיר/ה כי הנני מוסמך/ת לתת תצהיר זה בשם המציע.

א. השירותים והמועמדים המוצעים מטעם המציע נשוא מכרז זה זמינים ויועמדו לרשות המזמין מיידית ולאורך כל תקופת ההתקשרות ממועד החתימה על הסכם ההתקשרות ואילך.

ב. המציע מתחייב כי השירותים הכלולים בהצעה עומדים בדרישות הטכנולוגיות המפורטות במסגרת המכרז זה.

זה שמי, להלן חתימתי ותוכן תצהירי דלעיל אמת.

____________________	____________________	____________________
תאריך	שם	חתימה וחותמת

אישור עורך הדין

אני הח"מ ______________________, עו"ד מאשר/ת כי ביום _______________ הופיע/ה בפני במשרדי אשר ברחוב _______________ בישוב/עיר _______________ מר/גב' _______________ שזיהה/תה עצמו/ה על ידי ת.ז. _______________/המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

____________________	____________________	____________________
תאריך	חותמת ומספר רישיון	חתימה

מסמך זה הוא רכושה הבלעדי של מחב"א

נספח 1.6.9 תצהיר בדבר העדר תביעות והליכי פשיטת רגל

אני החי"מ _______________ ת.ז. _______________ לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

א. הנני נותן תצהיר זה בשם ___________________ שהוא המציע (להלן: "המציע") המבקש להתקשר עם עורך מכרז פומבי מספר 2-2023 שירותי IR\IRT למחב"א והמוסדות האקדמאים החברים בה. אני מצהיר/ה כי הנני מוסמך/ת לתת תצהיר זה בשם המציע.

ב. הריני להצהיר כי נכון ליום תצהירי זה____________ לא מתנהלות תביעות נגד המציע העלולות לפגוע בתפקודו במידה ויזכה במכרז והוא אינו נמצא בהליכי פשיטת רגל ו/או פירוק.

זה שמי, להלן חתימתי ותוכן תצהירי דלעיל אמת.

____________________	____________________	____________________
תאריך	שם	חתימה וחותמת

אישור עורך הדין

אני החי"מ _____________________, עו"ד מאשר/ת כי ביום ____________ הופיע/ה בפני במשרדי אשר ברחוב ____________ בישוב/עיר ____________ מר/גב' ______________ שזיהה/תה עצמו/ה על ידי ת.ז. ____________ /המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

____________________	____________________	____________________
תאריך	חותמת ומספר רישיון	חתימה

נספח 1.7 מפל – ניקוד איכות

מפ"ל - מפרט פנימי לבדיקה - מכרז IRT					
מספר	**דירוג סעיף**	**סעיף במכרז**	**דרישה**	**כמות**	**ניקוד**
1	S	1.6.4.3	עמידה בדרישות SLA בפריסה גאוגרפית לאזורים EX1, EX2	עמידה בדרישות SLA לאיזורEX1	4
				עמידה בדרישות SLA לאיזור EX2	2
2	S	3.1.3	תהליך חקירה, טיפול והכלת אירוע (תהליך מפורט)	פירוט תהליך והתחייבות לתהליך מתודי מפורט המכיל במינימום את כל השלבים המפורטים במכרז	12
3	S	3.1.4	תהליך התנעה מול מוסד אקדמאי	פירוט תהליך והתחייבות לתהליך מתודי מפורט המכיל במינימום את כל השלבים המפורטים במכרז	8
4	S	3.1.5	פריסת כלים ומנגנונים שונים	פריסת כלים אנליטיים לפני/בשלב אירוע (נדרש פירוט)	11
5	S	3.1.6	הדרכות והעשרות	ביצוע הדרכות בתכולה ובהיקף המינימלי המפורט במכרז	5
6	S	3.1.7	השתתפות בסימולציות	השתתפות בסימולציות בתכולה ובהיקף המינימלי המפורט במכרז	6
7	S	4.1	מודל "החופש האקדמאי"	ניסיון בניהול אירוע/הכלת אירוע במוסד אקדמאי (בשנתיים האחרונות)	5
				ניסיון בניהול אירוע/הכלת אירוע במוסד אקדמאי (לפחות 3 אירועים בשנתיים האחרונות)	5
8	S	5.1	אופן חקירת אירוע - מתודולוגיה	פירוט תהליך והתחייבות לתהליך מתודי מפורט בהתבסס על מתודולוגיה מוכרת ומתועדת, צירוף מסמך מתודולוגיות חקירה של הספק	6
9	S	7.1	יצירה/השבחה של נהלי IR ופרוטוקולי תגובה/בלימה	ניסיון מוכח ומתועד בכתיבה של נהלי IR/IRT צירוף דוגמאות	5
10	S	7.3	תיאור ותיוג אירועי ואיומים	תיוג מתודי של אירועים ואיומים - צירוף דוגמאות	6
11	S	7.4	פרוטוקולים להכלה ובלימת אירוע	יש לספק דוגמא לפחות ל 3 פרוטוקולים להכלת אירוע (מתוך הרשימה בסעיף 6.6)	6
12	S	7.6	מטריצת איומים מינימלית	התחייבות ל IR Play Book המכיל לפחות את הרשימה המפורטת במכרז (עד 15 תרחישים, מינימום 9 תרחישים)	5
				התחייבות וניסיון לכתיבת IR Play Book המכיל לפחות את הרשימה המפורטת במכרז (16 תרחישים ומעלה)	6
13	S	7.8	הפעלת נוהל DFIR לשמירת רצף עדויות ושימור מידע פורנזי	עמידה בתהליך DFIR לרבות שימור ראיות ושימוש בנוהל COC, התחייבות ופירוט אופן היישום של שלל התהליכים המפורטים	8

נספח 1.9 הסכם התקשרות

מצורף כמסמך נפרד

נספח 11 - מענה כספי

			מוסד אקדמאי בינוני			מוסד אקדמאי גדול		
מספר תכולה	שירות	תכולת שירות	עלות חד פעמית	עלות לשנה	עלות ל 3 שנים	עלות חד פעמית	עלות לשנה	עלות ל 3 שנים
1	תהליך התנעה On-Boarding ובניית תיק אתר **A**	כמפורט בסעיפים 3.1.8 ו 3.14		לא רלוונטי	לא רלוונטי		לא רלוונטי	לא רלוונטי
2	שירות IR/IRT מלא במודל ריטיינר **B**	כל תכולת השירותים הנכללת במכרז	לא רלוונטי			לא רלוונטי		
3	מחיר לשעת עבודה	מחיר לשעת עבודה בפעילות IR עד 199 ש"ע		לא רלוונטי	לא רלוונטי	לא רלוונטי	לא רלוונטי	לא רלוונטי
4	מחיר לשעת עבודה **C**	מחיר לשעת עבודה בפעילות IR -200 499 ש"ע		לא רלוונטי	לא רלוונטי	לא רלוונטי	לא רלוונטי	לא רלוונטי
5	מחיר לשעת עבודה	מחיר לשעת עבודה בפעילות IR 500 ש"ע ומעלה		לא רלוונטי	לא רלוונטי	לא רלוונטי	לא רלוונטי	לא רלוונטי

- מוסד אקדמי בינוני – אוניברסיטאות אריאל, בר אילן, הפתוחה, חיפה ומכון ויצמן
- מוסד אקדמי גדול – אוניברסיטאות העברית, תל אביב, בן גוריון והטכניון

החלוקה נעשתה בהתאם למפתחות התקצוב של ות״ת (הועדה לתכנון ותקצוב של המועצה להשכלה גבוהה)

נספח 12 – תמחור שירותים אופציונאליים

שירותים משלימים/אופציונליים					
מספר תכולה	**שירות**	**תכולת שירות**	**יחידת תמחור**	**מחיר**	**הערות**
1	יום הדרכה	יום הדרכה טכנית בתחום שיטות חקירה/פורנזיקה/הכלת אירוע/אכיפת בקרות/מודיעין - הדרכה באתר הלקוח ל 15 משתתפים כולל חומר לימוד מודפס	מחיר ליום		קורס יבוצע בגוש דן
2	קורס הדרכה בסיסי	קורס הדרכה טכנית בתחום שיטות חקירה/פורנזיקה/הכלת אירוע/אכיפת בקרות/מודיעין - הדרכה באתר הלקוח ל 15 משתתפים כולל חומר לימוד מודפס	מחיר לקורס (5 ימים)		קורס יבוצע בגוש דן
3	קורס הדרכה בסיסי	קורס הדרכה טכני בסיסי - מבוא לאיומים, שיטות מחקר, יכולת בלימת איומים - הדרכה באתר הלקוח ל 10 משתתפים כולל חומר לימוד מודפס	מחיר לקורס (5 ימים)		קורס יבוצע בגוש דן
4	כתיבת נוהל "מענה לאירוע משבר סייבר ומעורבות הנהלה"	כתיבת נוהל כולל התאמה נקודתית למוסד האקדמאי ושילוב מעורבות הנהלה, בקרות ושיטות	כתיבת נוהל מלא		
5	ביצוע תרגילי סימולציה אירוע סייבר Red/Blue Team לאנשי אבטחת מידע	תרגיל סימולציה יומי ל 10 משתתפים כולל הקמת סביבות, הכנת מסמכים תומכים ותשתיות והפקת דו"ח מסכם ליווי של לפחות 3 מנחים/מדריכים	מחיר לתרגיל יומי		
6	ניהול מו"מ תוקפים - שירות ריטיינר	הקצאת מנהל מו"מ ועמידה בכל התכולות והדרישות המופיעות בסעיף 8 ו 9	מחיר ריטיינר לזמינות 24x7x365		
7	ניהול מו"מ תוקפים - שירות לפי קריאה	הקצאת מנהל מו"מ ועמידה בכל התכולות והדרישות המופיעות בסעיף 8 ו 9	מחיר לשעה		
8	ביצוע תרגיל סימולציה אירוע סייבר משולב הנהלה	תרגיל סימולציה יומי לחברי הנהלה מבוסס תרחישים, דילמות, ליווי מקצועי, הכנת כל התשתיות ותכני התרגיל, הפקת דו"ח מסכם	מחיר לתרגיל יומי		