מפרט טכני

עבור מכרז 202/2020 לאספקת מערכת הפצת מסרוני SMS ושירותים מקצועיים

1. תיאור כללי

1.1. משטרת ישראל מבקשת לקבל מערכת לשליחת מסרוני SMS , לרבות תוכנה ורישיונות למערכת וכן שירותי תמיכה ושירותים מקצועיים תוך השתלבות במערך הקיים של משטרת ישראל.

1.2. השירותים במכרז זה נועדו לאפשר לארגון, ליחידות סמך ולמשתמשים נוספים לשלוח מסרונים באמצעות המערכת המוצעת.

1.3. הספק הזוכה יתחייב לספק את המערכת ולהתקינה, וכן לספק שירותי תמיכה, תחזוקה, שדרוגים, הדרכה ושירותים מקצועיים נלווים למערכת לכל אורך תקופת ההתקשרות.

1.4. המערכת המוצעת תהיה על בסיס מוצר מדף קיים.

1.5. הספק הזוכה יקנה לארגון ולמי מטעמו רישיון שימוש עולמי במערכת, בלתי הדיר ובלתי מוגבל בזמן , במספר המשתמשים בה, במספר התקנותיה ולביצוע פיתוחים עתידיים בה.

1.6. פירוט השירותים המבוקשים במכרז הם כדלקמן:

א. אספקת מערכת שליחת SMS .

ב. תמיכה, תחזוקה ושדרוגים למערכת.

ג. שירותים מקצועיים שונים.

ד. הדרכת משתמשים.

2. דרישות טכניות:

2.1. הספק מתחייב לספק את המערכת המוצעת ולהתקינה באתר הספק כשהיא עומדת בכל הדרישות המפורטות במפרט זה.

2.2. הספק מתחייב לספק מערכת מסרונים (SMS), אשר מאפשרת ניהול ושליחת מסרוני SMS לטלפונים ניידים עם גישה לכל רשתות התקשורת הקוויות והמובייל במדינת ישראל התומכות במסרונים.

2.2.1. המערכת תותקן באתר הספק.

2.2.2. תפעול המערכת יתבסס על שירותים מקוונים כמפורט בהמשך.

2.2.3. המערכת תחולק לשתי סביבות:

2.2.3.1. סביבה מאובטחת: באתר הספק שתחובר לרשת המבצעית המשטרתית ע"י רכיבי אבטחת מידע משטרתיים ,סביבה זו תחובר אך ורק למשטרת ישראל ללא חיבור לאינטרנט וללא חיבור ללקוחות אחרים של הספק.

הסביבה המאובטחת תכלול את הרכיבים הבאים:

א. FW

ב. שרתי WEB בתצורת NLB

ג. שרת בסיס נתונים עצמאי אך ורק לפרויקט זה.

ד. סביבת DR מלאה לסביבה המאובטחת .

2.2.3.2. דרישות טכניות של הסביבה המאובטחת:

א. על שרתי האפליקציה להיות מותקנים ע"ג מערכת הפעלה Windows Server 2019 / גרסת Linux עדכנית

ב. על שרת ה DB להיות מותקן בתצורה שרידה, כזו שתאפשר רציפות תפקודית בזמן תקלה בשרת

ג. על השרתים להיות מותקנים ע"ג תשתית וירטואלית המאפשרת HA לצורך שרידות מירבית

ד. על חומרת השרתים (ככל הניתן) ותשתיות התקשורת והאחסון להיות כפולות לטובת שרידות במקרה של כשל באחד מרכיבי החומרה

ה. על השרתים להיות מגובים. על הגיבוי להכיל גיבוי למערכת הפעלה, אפליקציה, בסיס נתונים וקבצי מערכת חיוניים אחרים ולהשמר באתר הספק למשך 60 ימים לפחות

2.2.3.3. סביבת אינטרנט: שיכולה להיות משותפת עם לקוחות אחרים של הספק , הסביבה תהיה מאופשרת אך ורק בפרוטוקול https

2.2.4. המערכת תכלול ממשק ניהול באמצעות דפדפן אינטרנט .

2.2.5. תמיכה בשליחה למספר זהב - מספר לקבלת הודעות נכנסות

2.2.6. תמיכה בקבלת תשובה ממקבל ההודעה

2.3. **דרישות פונקציונליות כלליות**

2.3.1. המערכת תתמוך פונקציונאלית בכל דרישות החוק והתקנים המחייבים, לרבות דרישות בדבר התאמה למכשירי קצה שונים.

2.3.2. תמיכה מלאה בריבוי שפות – שמאל-ימין וימין-שמאל – כולל עברית, אנגלית, ערבית, רוסית ואמהרית.

2.3.3. תמיכה בניוד מספרי טלפון נייד MNP (Mobile Number Portability)

2.3.4. <u>חיבור ופירוק מסרונים</u> - בחלק מהרשתות (GSM) ניתן לאחד מספר מסרונים למה שנראה כהודעה רציפה אחת .ככל שניתן ברשת התקשורת הרלבנטית ,על המערכת לאפשר בניית הודעות ארוכות לכיוון המשתמש וכמו כן יכולת לחבר חזרה הודעות ארוכות שמגיעות ממכשיר סלולארי (ומגיעות כיותר ממסרון יחיד.

2.3.5. על המערכת לאפשר תקשורת דו כיוונית באמצעות מסרוני SMS.

2.4. **יכולות ניהול**

2.4.1. המערכת תאפשר ניהול של משתמשי המערכת כולל:

2.4.1.1. יכולת ליצור משתמשים בכל הרמות – הן משתמשים המנויים והן מנהלי המערכת (להלן: "משתמשים מורשים") בתפקידים שונים.

2.4.1.2. יכולת להוסיף/לחסום משתמשים.

2.4.1.3. יכולת הקצאת הרשאה למשתמש מורשה בהתאם לנדרש (לדוגמה: רמת מנהל מערכת– שליטה מלאה; רמת מנהל ארגון – שליטה רק בתחום הארגון כולל אפשרות לכל אחד מלקוחות הספק להקים חשבון ולנהל משתמשים וקבוצות; רמת משתמש מורשה – שליטה לפעולות המשתמש הרשום בלבד.)

2.4.1.4. יכולת ניהול מכסות שימוש, ברמת המשתמש המורשה ובכלל זה יכולת קביעת מכסת פריטים יומית ,חודשית או קבועה לכל משתמש ,כולל אפשרות משלוח התרעה על התקרבות לסיום המכסה .

2.4.1.5. למערכת תהא יכולת לשלוח הודעת בדיקה.

2.5. **דו"חות ודיווחים נדרשים**

2.5.1. כל פעולה המתבצעת במערכת תירשם ביומן המערכת (LOG) . בין השאר יירשמו הפרטים הבאים:

2.5.1.1. תוכן הפריט.

2.5.1.2. שולח הפריט.

2.5.1.3. תאריך ושעת השליחה.

2.5.1.4. חיווי פתיחה/קריאה.

2.5.1.5. מספר היעד/כתבות מייל.

2.5.2. המערכת תנהל לוגים מלאים על תקלות משלוח.

2.5.3. המערכת תאפשר הפקת דו"חות מפורטים באון ליין, כולל דו"חות לפי תאריכים ופרמטרים שונים (כגון תוכן ההודעה, תאריך המשלוח, יעד), מספר/מייל, חיווי על הגעת ההודעה למכשיר הקצה ובכלל זה סטטיסטיקות במהלך תקופה מבוקשת, ואפשרות שמירת היסטוריה.

2.5.4. המערכת תאפשר חיוויים והתרעות מבוקשים – יכולת דיווחים והתרעות מרכיבי המערכת באמצעות פרוטוקולי SNMP, SMTP ו-SYS LOG ובאמצעות מערכות NMS שונות, לרבות:

2.5.4.1. רישומי התרעה של מערכת ההפעלה.

2.5.4.2. אירועי אבטחת מידע.

2.5.4.3. אירועי המערכת כולל חיווי סטאטוס משלוח ההודעות- האם הגיעו/לא הגיעו ומה הסיבה.

2.5.4.4. חיווי עבור תקינות המערכת ברמת SMTP, WS וכד'.

2.5.4.5. קבלת delivery reports מלאים לגבי משלוח הודעות ישירות באמצעות ה-Gateway.

2.5.4.6. קבלת מערכת דיווח מלאה, כולל סטטיסטיקות .

2.5.4.7. אפשרות צפיה בכל פריט (מסרון/דיוור וכד') נכנס או יוצא וכן בכל פריטים לפי משתמש ו/או תאריך/שעה ו/או קידומת מובייל/מייל ו/או ספק תקשורת.

2.5.4.8. המערכת תאפשר הפקת דו"חות וגרפים של כמות פריטים לפי טווח תאריכים ושעות – שנה ,חודש, יום מסוים, שעה ביום וכדומה.

2.5.4.9. המערכת תאפשר הפקת דו"חות על רישום משתמשים המאשרים קבלת דיוור.

2.6. **ממשקי המערכת**

2.6.1. המערכת תאפשר לכל משתמש מורשה ,בכפוף להרשאות להפיץ הודעת SMS במספר ממשקים:

2.6.1.1. כל הקריאות לממשקים יהיו בצורה חד סטרית - **<u>מכיוון המשטרה לכיוון הספק</u>** .

2.6.1.2. ממשק SMTP.

2.6.1.3. ממשק API - REST/WS - שימוש ב API עבור ממשק למערכת באמצעות web service התומך בכל תקני ה- (soap + rest) (לפי תקן Web Services Security העולמי ובהתאם להנחיות הארגון)

2.6.1.4. רשימת השירותים שיש לממש ברמת ה- SMTP / API

2.6.1.4.1. שירות שליחת הודעות עם פרמטרים: מטרת השירות הינו שליחת מסרונים עם יכולות הבאות:

2.6.1.4.1.1. מספר מזהים חד, חד ערכיים משטרתיים למסרון.

2.6.1.4.1.2. שליחה עתידית.

2.6.1.4.2. שירות שליפת סטאטוס הודעות עם פרמטרים: מטרת השירות הינו קבלת חיווי אודות המסרון שנשלח . שירות זה יבוצע בטכנולוגיה של polling עם יכולות הבאות:

2.6.1.4.2.1. הגבלת כמות הודעות בשליפה

2.6.1.4.2.2. שליפה רק למספרי זהב

2.6.1.4.2.3. המידע שחוזר יכיל את הנתונים:

2.6.1.4.2.3.1. מזהה חד, חד ערכי משטרתי.

2.6.1.4.2.3.2. סטאטוס.

2.6.1.4.2.3.3. תוכן ההודעה

2.6.1.4.2.3.4. חברת תקשורת.

2.6.1.4.3. שירות שליפת הודעות שהתקבלו - מטרת שירות הינו אחזור של הודעות שנשלחו.

2.6.1.4.4. שירות לבדיקת סטאטוס של מספר סלולרי, מטרת השירות לתת מידע אודות מספר סלולרי , האם ניתן לשלוח מסרון אליו ובאם לא מה הסיבה (לדוגמא , מספר סלולרי חסום ע"י חברת סולארי מסוימת) .

השירות יקבל כפרמטר מספר טלפון. המידע שחוזר יכיל את הנתונים:

2.6.1.4.4.1. סטאטוס קו/מכשיר

2.6.1.4.4.2. סטאטוס קבלת הודעה

2.6.2. המערכת תאפשר הפצת הודעות אוטומטית בהתאם לכללים מוגדרים מהתרעות המתקבלות באמצעות ממשקים ממערכות שונות ובכלל זה ממערכת Notification של שירות הזדהות בטוחה (זה"ב) לניהול זהויות וגישה לשירותים, ממערכות הניטור ואבטחת מידע, ניהול הזהויות וכדומה.

3. דרישות אבטחת מידע

על הספק הזוכה ועל המערכת לעמוד בדרישות אבטחת מידע הבאות:

3.1. כללי

3.1.1. הספק/נותן השירות – ובכלל זה ספקי משנה וכל המעורבים בהתקנת המערכת ו/או איזה מרכיביה, הקמתה ותחזוקתה - יעמוד בכל דרישות אבטחת המידע והגנת הסייבר.

3.1.2. הספק ידאג לאבטחת כל המידע אשר יגיע אליו.

3.1.3. המערכת תותקן בחצרי הספק– בין אם באתר הראשי ובין אם גם באתר ההתאוששות מאסון - אתר ה-DR (Disaster Recovery) ובין באתר אחר.

3.1.4. המערכת, על כל רכיביה, יכולה להיות מבוססת על תצורת ענן, אך ורק אם שרתי האירוח (לרבות אתר ה-DR) נמצאים בתחום מדינת ישראל.

3.1.5. אם קיים ונדרש מסיבה כלשהי התקנת רכיבי המערכת באתרי משטרת ישראל, הגישה אליהם תתבצע ממתקני משטרת ישראל בלבד ולא תתאפשר גישה מרחוק לשרתים או לאיזה מרכיבי המערכת.

3.1.6. המערכת תאפשר ביצוע פעולות וגישה לנתוני המערכת אך ורק לאותם משתמשים מורשים וברמות ההזדהות כפי שיוגדרו על ידי הארגון .

3.2. **תפישת האבטחה**

3.2.1. המערכת תעמוד בעקרונות הגנת הסייבר ואבטחת המידע במטרה להבטיח את הרציפות התפקודית, בהיבטים הבאים:

3.2.1.1. אמינות המערכת והמידע

3.2.1.2. זמינות המערכת והמידע

3.2.1.3. סודיות המידע, לרבות נתוני המערכת

3.2.2. בהתקנת המערכת ובמתן השירותים, הספק יישם את העקרונות הבאים מול ממשקי הניהול ושאר ממשקי המערכת:

3.2.2.1. אמצעי הזיהוי Identification

3.2.2.2. אימות הזיהוי Verification

3.2.2.3. Authentication - תצורת רכיב הזהות וההזדהות בתהליך הכניסה לשירות ובמהלך הפעילות האופרטיבית.

3.2.2.4. Authorization – תהליך אשרור אלמנט הזהות וההזדהות בתהליך הכניסה לשירות ובמהלך הפעילות האופרטיבית.

3.2.2.5. Access control – בקרת גישה בהתאם לכל רכיב במערכת.

3.2.2.6. Reliability – מהימנות המידע.

3.2.2.7. Confidentiality – סודיות המידע, הגנה על מידע רגיש (הצפנה).

3.2.2.8. שלמות המידע -Data integrity

3.2.2.9. מניעת התכחשות Non-repudiation

3.2.2.10. תיעוד, רישום, ניטור Log, Audit, Monitor

3.2.3. מוצרי צד שלישי: במידה והזוכה מבקש לבצע שימוש במוצר של צד ג' כמו plug-in, מחלקות עזר, מוצרים משלימים וכו' , נדרש לקבל על כך אישור מראש ובכתב של נציג הארגון.

3.2.4. הספק מתחייב להשתמש במערכות הפעלה עדכניות (windows server 2016 ומעלה) המעודכנות בטלאי האבטחה העדכניים ביותר. הספק יישם מדיניות התקנת טלאים עיתית.

3.2.5. הספק יתקין שרת Firewall מול תשתיות הגישה למשטרת ישראל.

3.2.6. ספק יממש סגמנטציה והפרדה מיטבית בין הרכיבים השונים (WEBSERVER, DB וכד') של חלקי המערכת המספקים שרות למשטרת ישראל.

3.3. דרישות חוק, תקנות ותקני אבטחת מידע

3.3.1. המערכת תענה על דרישות אבטחת המידע ואחרות המפורטות בגרסתם ומהדורתם העדכנית ביותר של החוקים, התקנות והתקנים, ותתמוך בהן. מובהר כי הן על המערכת עצמה והן על הספק וכל מי שפועל מטעמו לעמוד בדרישות הנ"ל.

3.3.2. הנתונים הפרטיים של כלל לקוחות המערכת יהיו חסויים .

3.3.3. הזוכה יפעל על פי ההנחיות הבאות:

3.3.3.1. הנחיות אבטחת המידע ופיתוח מערכות מאובטחות של יחידות משטרת ישראל;

3.3.3.2. תהליכי Secured Development Lifecycle - SDL;

3.3.3.3. עקרונות פיתוח מאובטח של ארגון OWASP העולמי;

3.3.3.4. עמידה בדרישות תורת ההגנה של רשות ההגנה סייבר;

3.3.3.5. תקן רימון 5 של רשות ההגנה בסייבר- במידת הצורך ;

3.3.3.6. עמידה בהנחיות יה"ב – היחידה להגנה בסייבר;

3.3.3.7. עמידה דרישות הרשות להגנת הפרטיות (לשעבר רשות משפט טכנולוגיה - רמו"ט).

3.3.4. במידת הצורך ועל פי הנחיות נציג הארגון, המערכת תעמוד בדרישות התקנים המפורטים להלן ותתמוך בהם:

3.3.4.1. תקן אבטחת נתונים ISO 27001;

3.3.4.2. הנחיות אבטחת סייבר ISO 27032;

3.3.4.3. תקן הבטחת איכות ISO 9001

3.3.4.4. תקן אבטחת נתונים בענן ISO 27017 .

3.3.4.5. תקן אבטחת פרטיות בענן ISO 27018 .

3.4. הגנה לוגית

3.4.1. המערכת תותקן ותממש תצורת Front/Back עם הפרדה מלאה לשלוש שכבות (Tier 3) - תצוגה, שכבת הלוגיקה העסקית, מסד נתונים. אם נדרש רכיב ניהול, הוא ייבנה בנפרד בצד "האחורי" של המערכת.

3.4.2. ממשקי המערכת יהיו מודולריים. תתאפשר הפרדת ממשקים, כגון הפרדה מלאה בין ממשק המשתמשים לבין ממשק הניהול, ובין ממשקי הניהול עצמם וגם תתבצע הפרדת רשתות מלאה, כולל מיקרו-סגמנטציה.

3.4.3. מערכות ההפעלה והשירותים (services) של המערכת יוקשחו על פי נהלי הארגון.

3.4.4. ביצוע עדכוני תוכנה קריטיים: עדכוני מערכות הפעלה ועדכוני אבטחת מידע יתבצעו באופן סדיר ושוטף ובאישור נציג הארגון. הספק יוציא עדכוני האבטחה עבור המערכת ככל שתתגלה חולשה, או שיתבצע שיפור למצב הקיים. המערכת תתמוך בביצוע הורדת עדכונים שלא בחיבור ישיר לאינטרנט (Offline).

3.4.5. הספק יתקין תוכנות ניטור על שרתי המערכת.

3.4.6. הספק יתקין תוכנות הגנה על שרתי המערכת המשתנות מעת לעת לפי הצורך.

3.4.7. המערכת תאפשר הפעלת מנגנון למניעת ריבוי בקשות בכל חלק של המערכת שבו נוצר ו/או מאומת מידע.

3.4.8. הספק יבצע סקר קוד ובדיקות חוסן לכלל רכיבי המערכת באמצעות חב' אבטחת מידע המתמחה בתחום זה, לפחות פעם בשנה; הספק ילווה בדיקות סקר קוד ובדיקות חוסן שיבוצעו על ידם בהתאם לדרישת נציג הארגון. הדו"ח יועבר לנציג מ"י.

3.4.9. הספק מתחייב לתקן כל ליקויי / חולשה / פגיעות שימצאו.

3.4.10. נדרש כי תהליך הפיתוח בכל שלב ישולב במתודולוגיות ונהלים לפיתוח מאובטח – SSDLC (Secure Software Development Lifecycle)

3.4.11. על הספק לדאוג לשמור על קוד המקור של המערכת ורכיביה.

3.4.12. אין בהתקנת תוכנות צד ג' ועדכוני תוכנה על ידי הספק ו/או מי מטעמו, כדי לגרוע מאחריות הספק לתמוך במערכת כמפורט במסמכי המכרז.

3.5. רשת ותקשורת

3.5.1. הקישוריות בין הספק לבין משטרת ישראל תהיה באמצעות קו נל"ן.

3.5.2. כל התעבורה תהיה מוצפנת בפרוטוקולי הצפנה מסחריים כגון IPSEC, AES 256bit וכדומה.

3.5.3. התקשורת תתאפשר רק כפי שהוגדר בסעיף 2.3 במפרט.

3.5.4. כל סוגי המסרים ללא יוצא מן הכלל היוצאים/נכנסים למערכת המציע מ או אל רשת המשטרה יהיו בפורמט XML.

3.5.5. כל סוג מסר במערכת המציע יקבל תיאור מבנה של הסכימה בפורמט XSD לא יתאפשר העברת מסרים ללא תיאום מראש על המבנה .

3.5.6. על המערכת לתמוך בצד הספק, באפשרות ניטור המערכת באמצעות מערכות כגון IPS, WAF, DB-FW, IDS,SIEM-SOC, זיהוי ומניעת הונאה ונוספות.

3.5.7. גישה שרת (Server Side) לרשת האינטרנט הציבורי: לא תתאפשר גישה לשירותים ברשת אינטרנט מצד השרת.

3.6. מניעת דלף מידע

3.6.1. הזוכה יתקין ויתפעל אמצעים למניעת זליגת מידע מהמערכת , לגורמים שאינם מורשים על ידי משטרת ישראל. האמצעים המוצעים יפורטו ע"י המציע, כדלהלן:

3.6.1.1. מוצר DLP.

3.6.1.2. הקשחת מערכת ההפעלה בעמדות קצה.

3.6.1.3. מניעת גישה למדיה ו-USB בעמדות קצה.

3.7. ניטור, לוגים (קבצי חיווי) והתרעות על ידי המערכת

3.7.1. הלוגים יהיו זמינים לבחינת נציג הארגון על פי דרישה בכל עת.

3.7.2. כל פעולה חייבת להיות מתועדת ברשומה אבטחתית ולהישלח למרכז ניהול אירועים (SIEM) של הארגון.

3.7.3. המערכת תאפשר למנהלי המערכת, בהתאם להרשאתם, להגדיר מהם הרכיבים אשר הפעילות בהם תתועד בקבצי הלוג ובקבצי החיווי.

3.7.4. המערכת תאפשר יכולת העברת לוגים ל- SIEM בהתאם לסטנדרטים מקובלים כגון Syslog.

3.7.5. המערכת תתמוך בהצגה וניתוח של מגמות ושימושים (Trends & Usage) לאורך זמן.

3.7.6. המערכת תאפשר קבלת התרעות מהמשתמשים על ביצוע חשד לשימוש לא נאות / תקין בחשבון.

3.7.7. המערכת תאפשר "להעשיר" את המידע בלוג, לדוגמה: סוג המכונה, סוג מערכת ההפעלה , .וכיו"ב . User Agent

3.7.8. קבצי החיווי (לוג) במערכת יהיו מוגנים מפני גישה (צפייה, שינוי, מחיקה) לא מורשית ,ותישמר האפשרות לזהות גישה לא מורשית. המערכות יתריעו על ניסיון גישה/שימוש החורג מגבולות ההרשאות שניתנו.

3.7.9. לא יתאפשר ביצוע שינוי במידע שייאסף לאחר שנרשם (מניעת התכחשות).

3.7.10. אבטחת רשומות – על הספק להיות אחראי ולוודא שמידע אישי של מי מלקוחות המערכת לא ייחשף בפני גורמים זרים כמו גם בלתי מורשים .

3.7.11. על המערכת לנהל תהליך מובנה ומסודר של אחסון ומחיקה של רשומות.

3.7.12. כלל רכיבי המערכות השונות נדרשים לבצע Audit מלא על הפעילות המתבצעת בהם.

3.7.13. יש לתעד כל פעולה עם הרשאות מנהל על התשתיות השונות.

3.8. **ניהול הזהויות (Identity Management)**

3.8.1. על המערכת לתמוך במנגנון Single Sign On בכלל רכיבי המערכת.

3.8.2. על המערכת לשלוח ולהציג חיווי למשתמש על כל הזדהות/ שינויי למערכת (notification).

3.9. **<u>מענה לאירועי אבטחת מידע ו/או איום להתפרצות אירוע אבטחת מידע</u>**

3.9.1. הספק הזוכה יבצע בקרות אבטחת מידע שוטפות על המערכת לפחות פעם בשנה, על כלל רכיביה, על מנת לוודא עמידתו בדרישות אבטחת המידע.

3.9.2. הבקרות השוטפות יכללו בין היתר ניתוח ממוכן של נתיב הביקורת, ביצוע מבדקי חדירה תקופתיים, סקרי סיכוני אבטחת מידע, בדיקת אמינות הנתונים (Integrity), וכל בקרה עצמית אחרת הנדרשת בכדי להבטיח את עמידתו בביקורות אבטחת המידע אשר יבוצעו ע"י משטרת ישראל מעת לעת להבטחת עמידת המציע/הזוכה בהתחייבויותיו.

3.9.3. הזוכה יבצע בדיקות חדירה למערכת לפני הפיכתה למבצעית במשטרת ישראל ועל כל שינוי מהותי בפרויקט, לדוגמת שינויים/החלפת תוכנה, שינוי בטופולוגית הרשת של הזוכה, הוספת רכיבים מחשוב/תקשורת וכד'.

3.9.4. כל ממצאי הבקרות, ביקורות, סקרי הסיכונים, מבדקי חדירה וכד' יועברו לנציג משטרת ישראל.

3.9.5. בנוסף לאמור לעייל, יתחייב הזוכה לבצע בקרות ובדיקות אבטחת מידע לפי דרישת משטרת ישראל, בין אם לאור אירועים שונים, שדרוג מערכת, חשדות לאירועים, או בשל סיבה או צורך אחרים כלשהם.

3.9.6. משטרת ישראל או מי מטעמה, יוכלו על פי החלטתה לקיים מעת לעת ביקורות אבטחת מידע בהתאם לצרכיה.

3.9.7. הזוכה יתחייב לבצע סקר אבטחת מידע מקיף על המערכת בתדירות אשר תבטיח את בחינת כלל המערכות במחזוריות של לפחות אחת לשנה.

3.9.8. תיקון הליקויים אשר יימצאו בבקרות ובביקורות אבטחת המידע הללו יתוקנו לפי הלו"ז המוגדר להלן:

3.9.8.1. תיקון ליקויים קריטיים – יחל באופן מידי ויושלם תוך 4 ימי עסקים לכל היותר.

3.9.8.2. תיקונים מהותיים שאינם חשיפות קריטיות - יבוצעו תוך 20 ימי עסקים ויושלמו בהקדם האפשרי.

3.9.8.3. תיקון ליקויים שאינם מהותיים ואינם קריטיים - יתוקנו תוך 60 ימי עסקים לכל היותר.

3.9.8.4. תיקונים אשר יתברר על ידי הזוכה כי תיקונם יארך משך זמן ארוך יותר בשל נסיבות אובייקטיביות, ידון במשותף עם משטרת ישראל ותתקבל החלטה משותפת לגבי לו"ז לתיקון.

3.9.9. הספק מתחייב לדווח ולהתריע באופן מידי לנציג הארגון על כל ליקוי אבטחתי ו/או פרצת אבטחת מידע – או חשד לליקוי ו/או פרצת אבטחת מידע - הקיימת או מתגלה במערכת ו/או בתשתיות בהן פותחה המערכת וכן להציג יכולת הפחתת הפגיעות, או הסיכון לפגיעות, עד לתיקון מלא של הליקוי והסרת הפגיעות.

3.9.10. מבלי לגרוע מהאמור לעיל ,הספק מתחייב לתת מענה מידי לאירוע כנ"ל ו/או איום.

3.9.11. להתפרצות אירוע כנ"ל ופתרונות, במסגרת פרק זמן המוגדר בטבלת ה- SLA , עבור תקלה קריטית ,ובהתאם להגדרת האירוע, במקרה של איתור פרצות אבטחת מידע, או אל מול איומי אבטחת מידע.

3.9.12. במקרה של אירוע ברשת ו/או בתשתיות הספק, על הספק למסור לנציג הארגון כל מידע וכל חומר רלבנטי, לרבות הקבצים הפגועים ודיווח מלא על אופן התפשטותם ברשת.

4. נפחים, עומסים וביצועים

4.1. על המערכת לעמוד בביצועים של קצב שליחה\קבלה של 100 מסרונים לשנייה לזמן רציף של לפחות 20 דקות. במצב זה לא יהיה עיכוב של יותר מ- 0.5 שניות בGATEWAY (קצה לקצה) ללא תלות ביתרות \שרידות הנדרשת.

5. מימוש הפתרון

5.1. כללי

5.1.1. המערכת תותקן בחוות השרתים של הספק וכן בהתאם להנחיות הארגון במתקן ה-DR של הספק.

5.1.2. הספק יתקין את המערכת, וכן יגדיר הגדרות, בהתאם למסמכי המכרז ובהתאם להנחיות הארגון.

5.1.3. מימוש המערכת יכלול התממשקות למערכות משטרת ישראל באמצעות ממשק מכונה (API) לייצוא וייבוא נתונים בהתאם לדרישות הארגון מעת לעת.

5.1.4. הספק יתפעל את המערכת באופן שוטף ,מלא ועצמאי. על הספק לספק הדרכה למערכת שתקנה לצוותים המקצועיים את היכולות הנדרשות לתפעול המערכת .

5.1.5. הספק יספק שירותי תמיכה בתקופת האחריות והתחזוקה כמפורט במסמכי המכרז.

5.2. משתמשים

5.2.1. הארגון יגדיר את משתמשי המערכת המורשים מטעמו באופן עצמאי ללא מגבלת משתמשים .

5.3. ניהול הפרויקט מטעם הספק

5.3.1. הספק ימנה מנהל פרויקט מטעמו שאינו חלק מצוות נותני השירותים. מנהל הפרויקט יהיה נציגו של הספק וירכז את כל משימות הספק ודרישות הארגון במהלך תקופת ההתקשרות. מנהל הפרויקט יהיה אחראי על תיאום העבודות בין הגורמים השונים מצד הספק לבין צוות הניהול מטעם הארגון.

5.4. **צוות נותני השירותים מטעם הספק**

5.4.1. הספק מתחייב להקצות אנשים קבועים לאספקת השירותים (להלן: "צוות נותני השירותים"). הארגון רשאי שלא להסכים להצבתו של נותן שירותים מסוים או לדרוש את החלפתו ללא צורך במתן נימוק כלשהו .הספק אינו רשאי להחליף מיוזמתו מי מנותני השירותים מטעמו ללא הסכמת הארגון, מראש ובכתב .

5.4.2. במקרה של צורך בכניסה לאתרי ארגון בהם נדרש סיווג ביטחוני, מתחייב הספק להעמיד נותן/ני שירותים שהוא/הם בעל סיווג ביטחוני מתאים. כל אדם מטעם הספק שיעסוק במתן השירותים ויהיה בכך צורך, יהיה בעל סיווג מתאים שיקבע על ידי משטרת ישראל ויעבור הליך של בדיקה.

5.5. **לוח הזמנים והשלבים למימוש הפרויקט:**

5.5.1. לאחר קביעת זוכה, וכנגד הוצאת הזמנה, הזוכה יספק ויתקין המערכת, עד להפעלה בייצור, בהתאם ללוח הזמנים והשלבים הבאים:

5.5.2. **<u>תכנית עבודה ואפיון :</u>**

תוך 30 ימים קלנדריים ממועד ההזמנה הספק הזוכה יספק:

5.5.2.1. תכנית עבודה – תכנית עבודה למימוש הפרויקט בשלבים, תכנית גאנט המבוססת על שיטת PERT הכוללת לוחות זמנים מחייבים לביצוע כלל הפעילויות המתוארות

5.5.2.2. מסמך אפיון מפורט אשר יביא לידי ביטוי את כל ההגדרות הטכניות ודרישות אבטחת המידע הדרושות על מנת לממש את הפונקציונאליות הנדרשת על-ידי משטרת ישראל

5.5.2.3. אישור תוכנית העבודה והאפיון הטכני: יבוצע על-ידי נציג משטרת ישראל

5.5.3. **<u>התקנת המערכת:</u>**

תוך 90 ימים קלנדריים ממועד אישור תוכנית העבודה לכל המאוחר, הספק יספק את המערכת בהתאם לאפיון: הגדרת תצורת המערכת והתקנת המערכת עד להפעלתה המבצעית המלאה.

5.5.4. **בדיקות המערכת עד להפעלתה בייצור**

5.5.4.1. סביבות עבודה – הספק ינהל שתי סביבות עבודה נפרדות - טסט וייצור.

5.5.4.2. בדיקות איכות - הספק יבצע בדיקות איכות (מסירה) וימסור את המערכת, לאחר שסיים בהצלחה את הבדיקות.

5.5.4.3. הגשת תיעוד וקוד מקור: הספק ימסור לידי הארגון את כל קוד המקור עבור פיתוחים שפותחו עבור הארגון ותיעוד מלא, בגרסה דיגיטאלית ומודפסת, עד ולא יאוחר ממועד התקנת המערכת.

5.5.4.4. הדרכה: במהלך שלב זה, וכפי שיקבע בתוכנית העבודה ,הספק יבצע הדרכה למשתמשים וימסור מדריך למשתמש בגרסה דיגיטאלית ומודפסת.

5.5.4.5. בדיקות קבלה: יבוצעו על ידי משטרת ישראל.

5.6. **אפיון מפורט**

5.6.1. איפון מפורט של השירותים יוגדר מול הספק לאחר מועד הזכייה לא יאוחר מחודש מיום קביעתו כזוכה.

5.6.2. הספק יקיים פגישות מקצועיות עם נציגי משטרת ישראל ובסיומם יעביר לידי הארגון אפיון מפורט של המערכת (כולל אפיון טכנולוגי ותשתיתי).

5.6.3. צוות מקצועי מטעם משטרת ישראל יאשר את האפיון או יעביר הערות לתיקון. הספק יבצע את התיקונים הנדרשים ויעביר את האפיון המפורט לאישור משטרת ישראל לא יאוחר משבועיים מיום קבלת בקשת התיקון, עד לאישור סופי .

5.7. **אספקת המערכת והתקנתה**

5.7.1. הספק מתחייב לספק ולהתקין את המערכת, תוך 90 ימים לכל המאוחר, ממועד ההזמנה על-ידי הארגון כאמור לעיל, לרבות מכלול הרכיבים הנדרשים להקמה ותפעול של המערכת, כאשר היא במצב הפעלה תקינה בייצור כאמור להלן ,ובכלל זה:

5.7.1.1. חומרה: ההתקנה תתבצע על תשתית וירטואלית אשר תסופק על ידי הספק, כולל התקנת שרת ,תוכנות הפעלה, רכיבי תקשורת וציוד היקפי – על הספק לפרט מפרט מינימאלי ואופטימאלי, ובכלל זה מנגנון גיבוי.

5.7.1.2. תוכנה יישומית: אספקת שירותי המערכת והתאמות פיתוח, הנדרשות להפעלה מבצעית של המערכת, על פי האפיון שייערך בהתאם לאמור בסעיף 5.6 לעיל.

5.7.1.3. על הספק לדאוג להקצאת 5 מספרי חיוג מקוצר בעל 4 ספרות (לדוגמה המספר "זמין") אשר יהיו בשליטה ובבעלות של משטרת ישראל .

5.7.1.4. כל רכיב נוסף, הדרוש למימוש המלא של התחייבויות הספק לצורך תפעול מלא בסביבת הייצור של המערכת על פי מסמכי המכרז וחוזה ההתקשרות (כגון ממשק SMTP לשרתי הדואר, ממשק למערכות ההפצה של הודעות הSMS, ממשק REST/WS - API - שימוש ב API עבור ממשק למערכת באמצעות web service וכיוצא בזה).

5.8. **בדיקות**

5.8.1. **כללי**

5.8.1.1. במועד שיקבע בתוכנית העבודה, ימציא הספק תסריטי בדיקות מסירה (להלן: "תסריטי בדיקות המסירה") ו"תסריטי בדיקות קבלה (להלן: "תסריטי בדיקות הקבלה) "(תסריטי בדיקות המסירה ותסריטי בדיקות הקבלה יכונו ביחד: "תסריטי הבדיקות") לאישורו בכתב של הארגון, בהתאם להוראות שבמפרט זה

5.8.1.2. בתסריטי בדיקות המסירה , יפרט הספק את תיאור בדיקות המסירה אותן הוא עתיד לבצע במערכת, הרכיבים והאלמנטים הנבדקים והתהליכים אותם מתעתד הספק לבצע במסגרת כל אחת מבדיקות המסירה .

5.8.1.3. הספק יפרט בתסריטי בדיקות המסירה את הכלים לעריכה, לביצוע ולניהול הבדיקות (לרבות פירוט הכלים בהם יבוצע שימוש לצורך בדיקות הביצועים); את היעדים, המדדים והסטנדרטים ושאר התנאים אשר התקיימותם מהווה תנאי להצלחת בדיקות המסירה ,בהתאם לדרישות הארגון במסמכי המכרז, לרבות ומבלי לגרוע, כללי האומדן והנוסחות בהם ישתמש הספק על מנת לבחון את תוצאותיה ו/או הצלחתה של כל בדיקת מסירה .במסגרת תסריטי בדיקות המסירה, יכלול הספק תסריטי בדיקות קבלה מפורטים המקיפים את כל התרחישים הקיימים במערכת הנבדקים, לרבות ממשקים עם מערכות ותשתיות, ככל שישנן כאלו.

5.8.1.4. תסריטי הבדיקות יהיו כפופים לאישור משטרת ישראל .

5.8.2. **בדיקות מסירה**

כתנאי לאישור להתקנת המערכת בסביבת הייצור, וכחלק בלתי נפרד מביצוע התחייבויותיו על פי מסמכי המכרז, יערוך הספק, בנוכחות נציגי הארגון, על אחריותו ועל חשבונו ,בשלבים ובמועדים הקבועים לשם כך בתוכנית העבודה להקמת המערכת, את בדיקות המסירה (לרבות בדיקות עמידה בדרישות אבטחת המידע, כפי שהוגדרו במפרט תכולת שירותים זה) וזאת בהתאם לתסריטי בדיקות המסירה שאושרו על ידי משטרת ישראל. מובהר בזאת, כי לא יהיה בנוכחות נציגי משטרת ישראל ו/או בהוראה אשר תינתן על-ידיהם על מנת להטיל על משטרת ישראל אחריות כלשהי ו/או על מנת לגרוע מאחריותו של הספק על פי מסמכי המכרז לבדיקות המסירה וכן לתיקון ממצאי בדיקות הקבלה כמפורט להלן.

5.8.3. **בדיקות קבלה**

5.8.3.1. הארגון יהיה רשאי, על פי שיקול דעתו, לערוך בדיקות קבלה של המערכת בעצמו ו/או באמצעות צד שלישי מטעמו והספק יהיה מחויב בשיתוף פעולה מלא עם הארגון או עם צד שלישי זה. על אף האמור, הארגון יהיה רשאי, על פי שיקול דעתו הבלעדי, לוותר על ביצוע בדיקות הקבלה.

5.8.3.2. בדיקות הקבלה של המערכת ייעשו בהתאם לתוכנית הבדיקות שתאושר מראש על-ידי הארגון ועל פי המפורט לעיל, על בסיס תסריטי בדיקות הקבלה שהגדיר הספק ושאושרו על ידי הארגון. הספק מתחייב להעביר לארגון תסריטי בדיקות קבלה לאישור המערכת במועד שיקבע בתוכנית העבודה. תסריטי בדיקות הקבלה יכללו, לכל הפחות, את הנקודות באות:

5.8.3.3. עמידה בדרישות המכרז, בכל הסיכומים שיושגו עם הארגון ו/או מי מטעמו ובדרישות המפרט.

5.8.3.4. הגדרה של זמני תגובה סבירים, תוך תיאור המנגנון לבדיקתם תוך ציון כלים ממוחשבים לשם ביצוע הבדיקות

5.8.3.5. בדיקות הקבלה, ככל שיבוצעו, יבוצעו במתקני משטרת ישראל, בכפוף לקביעת הארגון.

5.8.3.6. הארגון רשאי בכל עת במהלך תקופת ההתקשרות ,לבדוק את המערכת בכל דרך שימצא לנכון, לרבות ביצוע Code Review, בדיקות נתונים, מבדקי אבטחת מידע וחדירות, מבדקי ביצועים וכיוצא באלו מבדקים כנדרש. הספק יסייע לארגון ו/או למי שזה יורה בעת ביצוע בדיקות אלה.

5.8.3.7. הספק יפעל באופן מידי לתיקון, שכתוב, שינוי בהתאם לכל ממצא/ הערה שיתגלו במהלך בדיקות הקבלה .

5.8.4. **בדיקות ביצועים**

5.8.4.1. ככל שהארגון ידרוש ,הספק מתחייב לבצע במערכת בדיקת עומסים לתיקוף יכולת המערכת לעמוד זמנית בדרישות העומסים והביצועים כפי שפורטו בסעיף 4 לפרק 2 לעיל.

5.8.4.2. הספק יספק תסריט המתאר את הבדיקה שתבוצע על ידו ,ולהשתמש בכלי בדיקה המאושר על ידי הארגון לביצוע הבדיקה. כלי הבדיקה יתמכו בבדיקות לכמות משלוחים שונים במקביל.

5.8.4.3. הספק ימציא את תוצאות הבדיקה כהוכחה מחייבת לעמידת המערכת בעומסים.

5.8.4.4. הבדיקה תתבצע במועד כפי שייקבע על ידי הארגון לקראת עליית המערכת לאוויר ויהיה נוכח בה נציג משטרת ישראל

5.8.5. **בדיקות אבטחת מידע**

5.8.5.1. הספק יעמיד את כל רכיבי המערכת לבדיקות אבטחת מידע - חדירות/חוסן (Penetration Tests) וסקר קוד (Code Review), על ידי צוות אבטחת המידע של משטרת ישראל. הבדיקות בפועל יתבצעו מאתר משטרת ישראל .

5.8.5.2. הבדיקות יתבצעו במועד כפי שייקבע על ידי הארגון, לקראת עליית המערכת לאוויר.

5.8.5.3. טיפול בממצאי הבדיקות – הספק מתחייב לטפל בכל הממצאים ובהתאם להנחיות שיועברו לו על ידי הארגון ולתקן כל הנדרש לצורך קבלת אישור עליה לאוויר.

5.8.5.4. המערכת תעמוד בכל דרישות הממונה על אבטחת המידע וכן בנהלי אבטחת המידע ונהלי משטרת ישראל, כולל בדיקות חדירות וחוסן וסקרי קוד תקופתיים. על הספק למנוע קיום כל פרצות אבטחת מידע ולטפל בהן מיד עם גילוין, כולל הסרה מהמוצר כל איומי אבטחת המידע ותיקון כלל הליקויים ככל שיהיו .

5.9. **אישור הארגון לתוכנית העבודה, לאפיון המפורט ולתסריטי הבדיקות (להלן: "מסמכי העבודה")**

5.9.1. לאחר שהספק הזוכה ימסור לארגון את תוכנית העבודה, האפיון המפורט ו/או את תסריטי הבדיקות (מסירה, קבלה, ביצועים וחוסן/חדירה), הארגון יודיע לספק, בכתב, בהתאם לשיקול דעתו הבלעדי, אם ברצונו לאשר את אותו מסמך ממסמכי העבודה המוצע על ידי הספק (במלואו או בסייגים) או לדחותו.

5.9.2. דחה הארגון איזה ממסמכי העבודה או אישר אותו בסייגים , הספק יתקן את המסמך על חשבונו, ויגישו לארגון, את אותו מסמך ממסמכי העבודה כשהוא מתוקן, בהתאם לסייגים ו/או להערות אותם ציין הארגון בהודעתו.

5.9.3. הארגון ימסור לספק את התייחסותו למסמך המתוקן, בשינויים המחויבים, וכך עד קבלת אישור מלא וסופי מהארגון לאותו מסמך ממסמכי העבודה.

5.10. **תקופת הרצה**

5.10.1. תקופת ההרצה תתחיל מיום עליית המערכת לאוויר ותסתיים לאחר הפעלת המערכת בייצור במשך חודשיים רצופים ללא תקלות (להלן: "תקופת ההרצה") ובכפוף לקבלת אישור הארגון על השלמת ההרצה לשביעות רצונו.

5.10.2. במהלך תקופת ההרצה הספק יהיה אחראי לליווי שוטף לנציגי הארגון בתפעולם את המערכת, וייתן את כל הסיוע הנדרש לתפקוד המערכת וביצוע השירותים, לרבות ביצוע כל התיקונים הנדרשים כפי שיידרש על-ידי הארגון או מי מטעמו.

5.11. **תיעוד**

5.11.1. הספק יספק את התיעוד הנדרש למערכת כאמור להלן בהתאם ובמועד לפי דרישות הארגון:

5.11.1.1. תיעוד תסריטי הבדיקות ותוצאותיהן.

5.11.1.2. תיעוד טכני לכל כלי החומרה והתוכנה, כולל קונפדרציות שרתים ומבנה הקבצים בשרת.

5.11.1.3. מדריך למשתמש בהתאם לתפקידים וכן מדריך לצוות התשתיות - תפעול היישום; מפורט כולל צילומי מסכים - לאחראים על תפעול המערכת והפצת ההודעות לסוגיהן, הקמת דפי נחיתה וסקרים ועל האחראיים לתפעול תשתיות המערכת.

5.11.1.4. תיעוד לגבי פיתוחים והתאמות שבוצעו על המערכת, לרבות תיקי תכנות וקוד המקור.

5.11.1.5. כל תיעוד שיידרש בעתיד לצורך תפעול שוטף, תשתיות והסבות.

5.11.1.6. הספק מתחייב לעדכן את התיעוד הטכני, תיעוד ומדריכי המערכת ותיקי התכנות בהתאם לכול שינוי במרכיבי המערכת.

5.11.1.7. הספק רשאי להוסיף על רשימת התיעוד הנדרשת.

5.12. **הדרכה**

5.12.1. הספק מתחייב לספק לארגון ולנציגיו הדרכה בסיסית על המערכת, עד לתום תקופת ההרצה. ההדרכה תכלול את כל הנדרש כדי שנציגי הארגון יוכלו לנהל ולתפעל את המערכת תפעול שוטף באופן עצמאי על ידי כוח אדם של הארגון. ההדרכה תכלול הדרכה לגבי ביצוע פיתוחים והתאמות, כך שהארגון יוכל לעשות כן באופן עצמאי אם ירצה בכך .

5.12.2. הספק יעביר קורסים לצורך הדרכת משתמשים מורשים של המערכת סה"כ כ-20 משתמשים והדרכת מפתחים ומיישמים של המערכת כ-50 מפתחים ומיישמים. היקפי ההדרכות והיקפי המשתמשים והמודרכים המפורטים הם הערכה בלבד. **הקורס יכלול את כל הנדרש כך שכל משתמש בהתאם לתפקידו יוכל לבצע תפקידו במערכת באופן מלא, ראוי ונדרש.**

5.13. **שירותי תמיכה :**

5.13.1. הספק יספק את השירותים המפורטים להלן (להלן: "שירותי התמיכה") במהלך תקופת האחריות. כמו כן, הספק יספק את שירותי התמיכה במהלך תקופת התחזוקה.

5.13.2. תחזוקת המערכת ובכלל זה אספקת והתקנה של מהדורות חדשות, ומתן הדרכה ותיעוד מלא אודותיהן, והכל עד להפעלתן המלאה בייצור, ולרבות עדכונים נדרשים למערכת לצור התאמה לגרסאות מכשירי קצה, מערכות הפעלה, סטנדרטים ותקנים חדשים, דפדפנים חדשים, וכן אספקת מהדורות וגרסאות חדשות, עדכונים ,patches וכדומה של המערכת וקיום מחויבויותיו במידה ויופסק יצור המערכת.

5.13.3. הספק יידרש להתאים את המערכת ותוצרי ההפצה, לגרסאות עתידיות של מערכת ההפעלה ו/או לגרסאות עתידיות של דפדפנים ו/או לגרסאות עתידיות של מכשירי מובייל .

5.13.4. ביצוע שינויים ושיפורים עתידיים כפי שידרשו מעת לעת על ידי הארגון .

5.13.5. ליווי ותמיכה בצוות היישום של הארגון ובכלל זה יעוץ בפתרון בעיות ויישום נכון של השירות פי דרישת הארגון ותמיכה טלפונית בצוות היישום של הארגון במידה ונדרש.

5.13.6. דיווח ומעקב - הספק ינהל רישום מסודר של כל הפניות ,יטפל בתקלות וידווח על הפתרונות לארגון. אחת לרבעון, יעביר הספק לארגון דו"ח של כל הפניות אל מוקד הסיוע שיכלול, בין השאר, את תיאור הבעיה וזמן הפתרון.

5.13.7. שירותי התמיכה יינתנו בהתאם לצורך כדלקמן:

הספק יעמיד לרשות הארגון קו טלפון, כתובת דוא"ל או וואטסאפ (להלן: "**מוקד תמיכה**") אליהם ניתן לפנות בכדי לדווח על תקלות:

5.13.7.1. היה והארגון הזמין רמת תחזוקה רגילה – הספק יפעיל מוקד התמיכה בשעות העבודה.

5.13.7.2. היה והארגון הזמין רמת תחזוקה מורחבת (להלן:" רמת תחזוקה מורחבת"), יפעיל את מוקד התמיכה בימים ראשון עד חמישי מן השעה 00:08 ועד לשעה 00:24 ובימי שישי משעה 00:08 עד לשעה 00:15.

5.13.7.3. מוקד התמיכה יטפל בטיפול בתקלות ,בעיות ובשאלות המדווחות ע"י משתמשי הארגון המורשים וכן יעוץ בפתרון בעיות של המוצר וההתאמות שבוצעו על ידו עפ"י דרישת הארגון, וכן טיפול בתקלות על פי דיווח ומתן פתרונות לבעיות הנובעות מתקלות על ידי אספקת תיקונים או פתרונות עוקפים, עד למתן פתרון מושלם.

5.13.7.4. במקרים של תקלות משביתות/קריטיות ,מחוץ לשעות העבודה, הספק ייענה לפניית הארגון ויתמוך בתקלה עפ"י דרישת הארגון בכל דרך נדרשת.

5.13.7.5. על הספק להתחייב לרציפות שימור הידע, ובכללה יכולות המערכת, ההתאמות, ארכיטקטורה ותשתיות נדרשות במפורט בבקשה להצעות זו.

5.13.7.6. במידה והספק הינו ספק מורשה של המוצר ,מובהר כי הספק מתחייב לספק את שירותי התמיכה למוצר ללא קשר להמשך פעילותו העסקית השוטפת והתקינה של יצרן המוצר. במקרה בו יוחלט על ידי יצרן המוצר להפסיק את התמיכה ברכיב מרכיבי המוצר, לא יהיה בדבר כדי לפטור את הספק מאחריות לספק על חשבונו רכיב ו/או תמיכה הזהים בטיבם ובאיכותם לרכיב המוצר אשר ייצורו ו/או התמיכה בו הופסקה על ידי יצרן המוצר.

5.13.7.7. הארגון שומר לעצמו את הזכות לבצע את שירותי התמיכה או כל חלק מהם באופן עצמאי.

5.13.8. **עדכון טכנולוגי:**

5.13.8.1. הספק מתחייב כי במקרה של עדכון גרסה, הוצאת דגם חדש, החלפת סידרה או הפסקת ייצור של פריטי ציוד, יעדכן הספק את הארגון בחידושים ובעדכונים.

5.13.8.2. בכל מקרה של שחרור גרסה מעודכנת/משופרת של איזה מרכיבי התוכנה המשולבים במערכת (כולל מהדורת Major release), יציע הספק לארגון לעדכן את הגרסה הקיימת ללא כל תמורה נוספת עבור התוכנה ו/או התקנתה, כאשר התקנת התוכנה/גרסה תתבצע על פי הנחיות הארגון ,גם בשעות חריגות וללא חיוב נוסף.

5.13.9. **הפסקת יצור של המערכת והציוד המוצעים:**

5.13.10. במקרה של הפסקת ייצור המערכת ו/או איזה מרכיביה ו/או מפרטי הציוד הכלולים בהצעת הספק, על ידי היצרן ,או במקרה של תכנון להפסקת ייצור כאמור ,יפנה הספק לארגון מידית עם היוודע לו המידע כאמור.

5.13.11. בכפוף לקבלת אישורו של הארגון, מראש ובכתב, יספק הספק, במקום המערכת, הרכיבים והציוד שייצורו הופסק ,מערכת, רכיבים וציוד שתכונותיהם זהות או עולות - על פי בדיקת וקביעת הארגון - על תכונות המערכת והציוד שבהצעת הספק ,וזאת ללא כל תמורה נוספת; המערכת, הרכיבים והציוד החלופיים יעברו תהליך אפיון, התקנה והטעמה ומותאמים להליך האפיון ,ההתקנה וההטמעה שעבר המוצר המקורי.

5.14. **תקופת האחריות :**

5.14.1. תקופת האחריות תימשך 12 חודשים החל מאישור הארגון להפעלת המערכת בייצור (להלן: "תקופת האחריות").

5.14.2. במהלך תקופת האחריות כאמור, יספק הספק, ללא תמורה, שירותי תמיכה למערכת והכל בהתאם למוגדר ולמפורט לעיל.

5.15. **תקופת התחזוקה :**

5.15.1. עם סיום תקופת האחריות, ימשיך הספק לספק שירותי תמיכה למערכת, וזאת עד לתום תקופת ההתקשרות כהגדרתה בחוזה ועל פי התמורה ויתר ההוראות והתנאים המפורטים והמוגדרים בחוזה, ולשביעות רצונו המלאה של הארגון, ובכפוף להוצאת הזמנה חתומה על ידי מורשי החתימה של הארגון ובכפוף לתנאי ההזמנה.

6. שינויים והתאמות

6.1. הזמנת שירותים נוספים – שינויים ושיפורים

6.1.1. לצורך ביצוע תוספות ,פיתוחים שוטפים, ייעוץ, אינטגרציה, שינויים ושיפורים למערכת וכן משימות מקצועיות הנדרשות להפעלה תקינה ושוטפת של המערכת שאינן נכללות ביתר התחייבויות הספק על פי מסמכי המכרז (להלן: "שו"שים"), יהיה הארגון רשאי להזמין מהספק, מעת לעת ועל פי שיקול דעתו הבלעדי, ביצוע שירותים כאמור ועל הספק לבצעם בהתאם להנחיות הארגון.

6.1.2. הספק מצהיר שיש לו הידע הדרוש לביצוע שו"שים, והוא מתחייב ששו"שים שיבצע יבוצעו על פי הוראות והנחיות היצרן ולא יפגעו במחויבות הספק והיצרן לתת אחריות למערכת, לציוד ולשירותים המבוקשים, וכי שו"שים אלה ישתלבו במערכת כך שלא יפגעו באיכותה ופעולתה לאחר ביצועם.

6.1.3. הארגון יהיה רשאי להזמין שו"שים מעת לעת בנוהל הזמנת שו"שים כמפורט להלן.

6.1.4. הספק יספק את השו"שים באמצעות צוות נותני השירותים, אולם הארגון יהיה רשאי לבקש כי הספק יעמיד נותני שירותים נוספים או אחרים לשם ביצוע שו"שים.

6.2. נוהל הזמנת שו"שים

שו"שים יוזמנו בהתאם לנוהל הבא:

6.2.1. מנהל ההתקשרות מטעם הארגון, יבקש מהספק להגיש הצעה לביצוע שו"ש. ההצעה תהיה מפורטת ותכלול את האפיון הנדרש לביצוע. הלוז לביצוע השו"ש, השפעות צפויות והשפעות אפשריות של השו"ש על המערכת ועל ביצוע יתר התחייבויות הספק, וכל דבר אחר אשר יתבקש על ידי מנהל ההתקשרות.

6.2.2. השו"ש יבוצע בהתאם להחלטת הארגון ועל פי שיקול דעתו הבלעדי, באחת מהדרכים הבאות:

6.2.2.1. או מחיר לפי שעה, בהתאם לביצוע השעות בפועל, או לחלופין - במחיר כולל בהתאם להצעת הספק כאמור בסעיף לעיל. במקרה של מחיר כולל, יסוכמו אבני הדרך לתשלום.

6.2.3. הצעתו של הספק תוגש למנהל ההתקשרות מטעם הארגון.

6.2.4. הארגון יהיה רשאי לפנות לספק בקשר לכל רכיב שנכלל בהצעתו ולבקש לגביו הבהרות / השלמות / עדכונים/ שינויים. יובהר, כי בכל שלב, רשאי הארגון לאשר או לדחות את הצעתו המעודכנת של הספק, לנהל משא ומתן נוסף ביחס אליה, או לשנות את שיטת ההתקשרות –והכל בהתאם לשיקול דעתו הבלעדי.

6.2.5. רק לאחר אישור בכתב של מנהל ההתקשרות את הצעתו של הספק (המקורית או המעודכנת), יוציא הארגון לספק הזמנה מתאימה החתומה כדין על ידי מורשי החתימה המוסמכים לחייב את הארגון.

6.2.6. הספק מאשר כי ידוע לו כי תחילת ביצוע השו"ש על-ידיו מותנית בהוצאת הזמנה מתאימה וחתומה כדין לביצוע השו"ש ובמילוי שאר ההוראות של סעיף זה וכי לא תהיה לארגון כל חובה לקבל את הצעת הספק.

6.2.7. הספק ינהל יומן עבודה מפורט בו יתעד את כל הפעולות שנעשו על ידו במסגרת מתן השו"שים לארגון. כן ינהל יומן ובו פירוט היקף שעות שו"שים שסופקו בכל חודש.

6.2.8. היה ובוצעו שו"שים במחיר לפי שעה ,כחלק מהדיווח החודשי של הספק ביחס לשירותים נשוא החוזה שסופקו על ידיו, יגיש הספק למנהל ההתקשרות מטעם הארגון לבדיקה ולאישור דו"ח מפורט הכולל גם ריכוז חודשי של ביצוע השו"שים הללו, לרבות פירוט שעות העבודה ורכיבים במידה והיו. דו"ח זה יוגש לבדיקה ולאישור של למנהל ההתקשרות מטעם הארגון כחלק מההתנהלות השוטפת של הספק לעניין דיווח ותשלום התמורה בגין השירותים.

6.2.9. התשלום עבור שו"שים במחיר כולל, יתבצע בהתאם לאבני הדרך המוסכמות.

6.2.10. כל שו"ש תימסר לבדיקות הארגון בהתאם לנהלים. כל משימה תעבור סדרת בדיקות מסירה של הספק בסביבת בדיקות. לאחר ביצוע בדיקות מסירה, ימסור הספק את השו"ש לארגון לשם ביצוע בדיקות קבלה, שיבוצעו על פי שיקול דעתו של הארגון. השו"ש יותקן בסביבת ייצור רק לאחר קבלת אישור בכתב מהארגון.

6.2.11. התשלום לספק יתבצע לאחר אישור בכתב של מנהל ההתקשרות לביצוע השו"ש לשביעות רצונו ואישור הדו"ח ובהתאם לנוהל התשלום הנוהג בארגון.

6.2.12. יובהר, כי הארגון רשאי לבצע משימות באופן עצמאי באמצעות בעלי תפקידים מטעם הארגון ,או באמצעות כל גורם אחר עמו יבחר הארגון להתקשר, וכי אין בנוהל האמור כדי לחייב את הארגון לפנות לספק בבקשה להצעות.

7. רמת שירות

הספק מתחייב לספק את השירותים בהתאם לכללים ולתנאים המוגדרים להלן:

7.1. **קריאה לשירות**

7.1.1. הספק מתחייב לקיים מוקד שירות עם מענה אנושי וטיפול בתקלות. זמן ההמתנה המקסימאלי למענה אנוש במוקד הסיוע לא יעלה על חמש דקות.

7.1.2. היענות לקריאת שירות - הספק יידרש לעמוד בזמני התגובה שמפורטים להלן באמנת השירות לקריאות שירות.

7.2. **מעקב ובקרת השירות**

7.2.1. כל קריאת שירות וטיפול בתקלה, תתועד על ידי הספק בזמן אמת. הספק יפיק "דו"ח תקלה" לאחר פתרונה אשר יכלול את תיאור הקריאה, תיאור התקלה, תיאור הפתרון.

7.2.2. לפי דרישת הארגון, ולכל הפחות אחת לרבעון גם אם לא נדרש לעשות כן על ידי הארגון, ימציא הספק דין וחשבון ובו –

7.2.3. פירוט קריאות השירות שטופלו על ידו.

7.2.4. תיאור כל קריאה והטיפול בה.

7.2.5. הדו"חות יוגשו לנציג משטרת ישראל הן בעותק קשיח והן בעותק רך.

7.3. **אמנת שירות (SLA)**

7.3.1. הספק מתחייב לעמוד בזמני התגובה שמפורטים להלן באמנת השירות לקריאות שירות ו/או תפעול ובהתאם מתחייב הספק על עבודה רצופה, שוטפת ומאומצת, במסגרת יום העבודה, תוך הקצאת מלוא כח האדם המתאים והנדרש עד לפתרון הבעיה.

7.3.2. חלון הקריאה לקבלת שירות, זמן התגובה לטיפול בתקלות, אופן הטיפול במוצרים ובציוד ומהות הכיסוי, ייעשו על פי המפורט להלן וכן על-פי כל התנאים המפורטים במפרט הטכני ובחוזה ההתקשרות.

7.3.3. על הספק לעמוד בזמני התגובה הבאים לקריאות שירות:

סוג התקלה	תיאור סוג התקלה	חלון שירות	זמן תגובה / זמן תחילת טיפול – דרישות המכרז
קריטית	משביתת מערכת	365*7*24	תחילת הטיפול בתקלה בתוך 1 שעה לכל היותר בשעות העבודה מרגע פתיחת הקריאה במוקד ותוך 3 שעות כאשר פתיחת הקריאה אינה בשעות העבודה. במידה ונדרשת הגעת אנשי המקצוע של הספק למתקן הארגון, זמן הגעה לאתר הארגון– תוך 3 שעות ממועד פתיחת הקריאה.
חמורה	משביתת שירות/ים או רכיב/ים במערכת או שימוש ביכולות המערכת	365*7*24	תחילת הטיפול בתקלה תהיה תוך 4 שעות מרגע פתיחת הקריאה במוקד. במקרה של דיווח לאחר השעה 18:00, הטיפול בתקלה יחל ביום העבודה הבא, עד השעה 09:00 בבוקר לכל המאוחר.

רגילה	אינה קריטית או חמורה		תחילת הטיפול בתקלה שדווחה עד השעה 12:00, תהיה באותו יום עד השעה 18:00. במידה ודווחה תקלה לאחר השעה 12:00, תחילת הטיפול בה תהיה ביום העבודה הבא עד 12:00 בצהריים.