נספח 5

דרישות תקשוב למרלו"ג משטרת ישראל

נספח 5 א' - מערכות תשתית ותקשורת מחשבים+טלפוניה - תשתית אחודה למשטרה בלבד

1. **מבוא**

1.1. המפרט להלן בנספח זה, מתייחס לאזורים ולפונקציות שבתפעול לוגיסטי של משטרת ישראל, ובכל מקום בו נדרש רשת תקשורת משטרתית (מחשבים וטלפוניה), לרבות:

1.1.1. משרדי חוליית הקישור למרלו"ג.

1.1.2. מעבדת סמים.

1.1.3. מתחם "צומת הדואר".

1.1.4. משרדי משטרת ישראל הממוקמים במתחם הבלאי, השיקום והגריטה.

1.1.5. בכל פונקציה נוספת שתדרש, כפועל יוצא של תפעול לוגיסטי בלעדי של משטרת ישראל.

1.2. בכל שאר אזורים במרלו"ג, יבצע הזוכה את מערכות התשתית על פי כל התקנים הרלוונטיים המקובלים בישראל ועל פי כל דין.

1.3. המפרט להלן מתייחס להקמה של מרכז לוגיסטי באתר חדש. במקרה של שימוש באתר קיים יבוצעו התאמות בתשתית הקיימת ויאושרו על ידי הגורמים המקצועיים במשטרת ישראל, בהתאם לגופו של כל מקרה.

1.4. התכנון והביצוע יאושרו על ידי משטרת ישראל.

2. **דרישות תשתית (שחורות) לתקשורת מחשבים**

2.1. הזוכה יתכנן ויתקין תעלת רשת לאורך המסדרונות ועפ"י התוואים הקיימים תעלת רשת בגודל מינימאלי של 8.5 X 20 ס"מ (גודל התעלה ישתנה בהתאם לכמות הכבילה אשר תיפרס באותו התוואי), התעלה תהיה מחוזקת לתקרה / רצפה (במידה ותותקן רצפה צפה) הקבועה באמצעות זוויות חיזוק או מוטות הברגה. התעלה תהיה ייעודית לתקשורת מחשבים והטלפוניה.

2.2. תעלות/ מעברים/ קידוחים עבור כבלי התקשורת ומתח נמוך לאורך המסדרונות ובפירים יהיו בגודל אשר יאפשר גידול כמות תשתיות התקשורת בכ- 30% לפחות.

2.3. מכל נקודת מחשב / טלפוניה יצא צינור 25 מ"מ מנקודת הקצה אל תעלת הרשת. הצינור יעוגן לתעלת הרשת בכיוון משיכת הכבל אל ארון התקשורת.

2.4. כל נקודת קצה תסתיים בקופסת חיבורים כדוגמת גיווס (4 מקומות לפחות) או עמדת עבודה משולבת כדוגמת סימה בוקס (דגם D-14,D-18,D-20).

2.5. אין להשתמש בצינורות שרשורים ובצינור הקטן מקוטר 25 מ"מ.

2.6. קידוח בין קומות במידה ויידרש, יאטם אחרי גמר השחלת הכבלים.

3. <u>דרישות בינוי לחדר תקשורת מחשבים</u>

עפ"י המלצת התקן הישראלי ובטיחות מערכות מידע, יש לשמור על הכללים הבאים:

3.1. יש להגן על פתחי החלונות החיצוניים, באמצעות סורגים או אמצעי אבטחה אחרים. כמו כן, יש להתקין אלמנטי הצללה בכדי למנוע חדירת קרני שמש לחדר, ולשפר את יכולת הקירור של המזגנים בחדר.

3.2. בכלל חדרי התקשורת תותקן מערכת בקרת כניסה וכן גלאי נפח, ע"מ לאפשר בקרת כניסה בשעות אי הפעילות. באחריות הזוכה ביצוע פריסת התשתית השחורה כולל התקנת מחזיר שמן ומנעול חשמלי. המערכת מתוכננת לשליטה מרחוק דרך רשת תקשורת משטרתי וחיבור למערכת גילוי פריצה במתקן. מצ"ב פרט עקרוני לביצוע והכנת תשתיות צנרת / מובילים עבור מערכת הנעילה של חדרי התקשורת בלבד (מופיע בסעיף 21). המערכת תותקן ע"י משטרת ישראל.

3.3. במידה ויותקנו לחדרי התקשורת דלתות מוגנות אש, על הזוכה לדאוג להתקנת דלת כולל כל האמצעים הנדרשים להתקנה מלאה.

בדלת יותקן מנעול - צילינדר חשמלי מתח עבודה DC V12, המנעול החשמלי יהיה מאושר מכון התקנים להתקנה בדלת אש.

תינתן אינדיקציה מהידית הפנימית עבור פתיחה חוקית, וכן אינדיקציה עבור זיהוי דלת פתוחה. הכבילה של כל המערכות תסתיים בתוך חדר התקשורת בחלל התקרה שמעל דלת הכניסה, יש לסמן את הגידים ובמידת הצורך להעביר למשטרה סקיצה ותוכנית של הדלת כולל מקרא לגידי הכבילה של המערכות שבדלת.

3.4. הקירות החיצוניים של חדרי \ ריכוזי התקשורת יבנו מקירות גבס דו קרומים הכולל בין השכבות פח מגולוון בעובי 2 מ"מ, או לחילופין קירות בלוקים, עמידות לאש למשך שעתיים.

3.5. הכניסות לחדר תקשורת מחשבים יהיו באמצעות דלת פלדלת. הדלתות תהינה מצוידות במנגנון סגירה אוטומטי (מחזיר שמן), פתח נטו בין משקופים 90 ס"מ.

3.6. עוצמת תאורה בחדר תקשורת מחשבים תהיה 800 לוקס לפחות. התאורה תותקן בגופים פרבולים T-5 דו-תכליתיים, הכוללים אמצעי הגנה בפני סנוור/ תאורת לד הכוללת גופים דו תכליתיים- גוון התאורה יהיה 3500 קלווין ומעלה. תאורת החדר תוזן ממעגלים חיצוניים, גופי תאורה ימוקמו בהתאם להעמדת הציוד בחדר.

3.7. בחדרי התקשורת תותקן רצפה רגילה כדוגמת הרצפה אשר תותקן בתחנה, למעט בתחנות בהם יותקנו חדרי תקשורת מרכזיים/ חדרי שרתים – בחדרים אלה תידרש התקנת רצפה צפה / ריצפת PVC אנטי

סטטית הכוללת פסי הארקה מתחת לרצפה והוצאת 4 קוצים להארקה בכל פינות החדר וחיבורם להארקה ראשית כולל קופסת מעבר- הנחיות ודרישות יוגדרו ע"י משטרת ישראל/מנ"ט/תקשוב

3.8. בכלל חדרי התקשורת לא יותקנו צינורות המובילים מים למערכות שונות המותקנות במבנה (כיבוי אש, ביוב, מזגנים ועוד).

3.9. שטח חדר תקשורת מחשבים ראשי: 15 ממ"ר.

3.10. מיקום מומלץ לחדר תקשורת המחשבים, יהיה ככל האפשר במרכז. רוחב מינימאלי לחדר התקשורת - 3 מטר.

4. **<u>דרישות לריכוז תקשורת משני/קומתי</u>**

4.1. בנוסף יש צורך בחדרי תקשורת קומתיים בשטח רצפה של לפחות 12 ממ״ר, אשר ישמשו לריכוז קומתי או כריכוז נוסף באותה הקומה וזאת בתנאי שאורך כבילה רצופה אינו עולה על 80 מ׳ מהריכוז הקרוב. בכל מקרה, כל שטחי התקשורת יאושרו ע״י משטרת ישראל לאחר קבלת תוכניות המתחם.

4.1.1. פתח נטו בין משקופים 90 ס״מ.

4.1.2. עבור כל ארון תקשורת נדרש להתקין שתי נקודות חשמל 16 A מלוח חשמל ייעודי משני שדות שונים (אפיון הלוח עפ״י פרק11) שיותקן בחדרי התקשורת וסיומו בשקע CEE מוזן לפני ממסר פחת מחיוני. יש לשלט באדום ״מוזן לפני ממסר פחת״ וכן מספר מעגל.

4.1.3. קו הארקה 16 ממ״ר, שיחובר להארקת יסוד.

4.1.4. התקנת תאורה דו-תכליתית בחזית ארונות התקשורת.

5. **<u>ארונות תקשורת</u>**

5.1. בכל חדרי התקשורת יספק הזוכה ארונות תקשורת בגדלים שונים ועפ״י מפרט טכני אותו תגדיר משטרת ישראל. בארונות אלה ייוצגו שקעי הקצה, ויתקנו בהם מערכות התקשורת, ציוד אקטיבי וכד׳. כמות ארונות התקשורת תהיה על פי תכנון ודרישת יועץ התקשורת של משטרת ישראל, לא עפ״י כמות הארונות המופיעה בתוכנית החשמל.

5.2. ארונות התקשורת יהיו מדגם לנטל, סוג וגודל ארונות התקשורת יהיה על פי תכנון ודרישת משטרת ישראל לרבות הזמנת ארונות 44U המחולקים (בחלוקה פנימית) למספר ארונות וכן הזמנת ארונות במידות עד 50U , כל זאת בהתאם לדרישות ועפ״י תכנון ואפיון שיועבר ע״י משטרת ישראל.

4.1 ארון התקשורת מיועד להתקנה של לוחות הניתוב ולהתקנה של ציוד תקשורת. דפנות הארון יהיו עשויות פח ופריקות. הארון יהיה עם דלת קדמית אחת, רשת קמורה. עם ידית ומערכת נעילה. מאחור (גב הארון) 2 דלתות פח מחוררות כולל נעילה, צבע הארונות יהיה לפי דרישת הלקוח, הארונות יסופקו עם רגליות / גלגלים.

4.2 מסילות התקנת הציוד / פנלים בארונות יותאמו לאומי כלוב.

4.3 ארונות התקשורת יסופקו עם 4 מאוררים, 2 פסי חשמל (N-12) כולל מאמ״ת A16, שקע הסיומת של פס החשמל יהיה מסוג CEE16A או תקע ישראלי וזאת לפי דרישת משטרת ישראל

4.4 לארון התקשורת תהיה נקודת הארקה אחת באמצעות קיט הארקה המתאים לחיבור האמצעים המותקנים בארון.

4.5 לארונות התקשורת יסופקו מדפים קבועים, מדפים נשלפים ומגירות שירות לפי דרישת משטרת ישראל

4.6 בארונות התקשורת יותקנו פנלי ניהול כבילה בגודל 2U לפי סטנדרט המשטרת ישראל לטובת העברת מגשרי התקשורת בארונות.

6. <u>שילוטים</u>

6.1. הזוכה יבצע סימון ושילוט של כל הפריטים המותקנים, על פי השיטה שתפורט להלן.

6.2. השילוט של כל פריט יבוצע במיקום, אשר יאפשר את קריאתו ללא צורך בהזזת פריט או פריטים סמוכים.

6.3. הכיתוב יהיה קריא, ברור ובלתי מחיק שילוט PVC חרוט.

6.4. צבע השילוט יועבר לידי הזוכה בשלב התכנון המפורט.

6.5. הפריטים אותם ישלט הזוכה הינם כלל חדרי התקשורת, חדר המרכזייה, כלל ארונות התקשורת, כלל לוחות הניתוב, פנלים אופטיים, שקעי קצה, גישורי נחושת, גישורי סיבים, על כלל הכבילה תודבק מדבקת שילוט.

7. <u>מגשרים</u>

7.1. משטרת ישראל תעביר רשימה של סוגי המגשרים לזוכה לטובת הפעלת מערך התקשורת.

7.2. כמות המגשרים תהיה 200% מכלל נקודות התקשורת אשר נפרסו באתר.

7.3. המגשר יהיה בתקן CAT6A לפחות באורכים וצבעים שונים לרשת תקשורת המחשבים ולפי החלטת משטרת ישראל

7.4. המגשר לרשת הטלפוניה (בצד חיבור מכשיר הקצה בלבד יהיה בתקן CAT6A או אחר עפ"י אפיון משטרת ישראל.

7.5. מגשר אופטי (MM\SM) התואם לסיבים אשר נפרסו באתר בסוגים שונים (SC,LC ועוד)

7.6. התקנים הרשומים בסעיפים הנ"ל מותאמים לתקופה הנוכחית במידה והתקינה תשתנה על הזוכה יהיה לספק מגשרים בהתאם לאותה תקופת זמן.

7.7. כמות המגשרים, אורכם וצבעם יועבר לידי הזוכה לקראת התכנון המפורט.

7.8. כל המגשרים יהיו משולטים במדבקה מתלפפת הכוללת: אורך המגשר ומספר רץ.

8. <u>מולטימדיה</u>

8.1. בחדרים מסוימים על פי החלטת משטרת ישראל תוכן תשתית מולטימדיה בהתאם לסטנדרטים של משטרת ישראל

8.2. התשתית תכלול נקודות חשמל, מפסקים, אמצעים חשמליים וכל הנדרש להפעלת מערכות החשמל של המולטימדיה. עבור כבילת המולטימדיה (מתח נמוך) הזוכה יתקין תשתית שחורה הכוללת צנרת / תעלות חיצוניות בלבד.

8.3. לקראת תכנון מפורט תועבר תוכנית פריסת תשתית המולטימדיה הכוללת צנרת, נק׳ חשמל, הארקה, מכלולי עבודה, ארון תקשורת ועוד.

8.4. מכל עמדת מולטימדיה יצאו 2 צינורות 29 מ״מ לפחות מעמדת הקצה אל תעלת הרשת / ריכוז המולטימדיה המקומי. הצינור יעוגן לתעלת הרשת בכיוון משיכת הכבל אל ארון התקשורת. הזוכה יניח חוט משיכה בצינור. בכל מקרה, על זוכה לקבע את הצינור ולחתוך את עודף הצינור בצורה שלא תפריע להתקנת עמדת המולטימדיה.

8.5. יש להקפיד שאורכי צנרת המולטימדיה שיפרסו בחדרי ישיבות, תדרוך וכד׳ לא יעלו על 12.5 מ׳ מנקודה לנקודה למעט חדרים גדולים (מעל 30 מ״ר) בהם משטרת ישראל תבצע התקנה של ציוד אקטיבי להרחקת מערכות המולטימדיה.

8.6. כל עמדת מולטימדיה תסתיים בקופסת חיבורים כדוגמת סימה בוקס (דגם D-11, D-20 17, D-D-14,D-18).

8.7. בחדרים בהם יותקנו ארונות מולטימדיה, תותקן בגב הארון קופסא CI (גודל הקופסא יקבע לפי כמות הצנרת אשר תותקן בחדר) לצורך ריכוז צנרת המולטימדיה אשר תיפרס בחדר.

8.8. בחדרים אשר יותקן ארון מולטימדיה ואמצעי מולטימדיה אחרים תועבר דרישה למיקום נקודות החשמל, מפסקים ופריסת הצנרת הנדרשת.

9. <u>גילוי אש</u>

9.1. יש להתקין מערכת גילוי אש בכל מערך חדר תקשורת המחשבים.

9.2. בחדרי התקשורת תותקן מערכת כיבוי אש המערכת תותקן בשטח החדר, והצנרת של המערכת תותקן מעל התקרה האקוסטית.

9.3. במידה ובחדר התקשורת תותקן רצפה צפה, תותקן מערכת כיבוי בגז בחלל הרצפה.

9.4. יש לבצע איטומים מתאימים בחלל התקרה לשמירת חלל סגור ואטום.

9.5. ניתן להתקין את בלון הכיבוי בגז של חדר התקשורת בתוך חדר התקשורת, יש לוודא עיגון של הבלון והתקנת מנגנון הפעלה מחוץ לחדר, כולל נפץ חשמלי ייעודי. – מיקום התקנת בלון הכיבוי יעשה בתאום עם יועץ התקשורת של המשטרה. באחריות הזוכה לוודא שהתקנת הבלון והצנרת מבוצעת תוך פגיעה מינימלית בתשתיות הקיימות בחדר התקשורת ובחלל התקרה.

9.6. מערכת הכיבוי תהיה בגז (FM – 200), גודל מיכל הכיבוי ייקבע בהתאם לגודל החדר ולפי הנחיות יועץ הבטיחות של הזוכה.

9.7. יציאה לניתוק חשמל בחדר ללוח ומזגנים, במצב כיבוי בלבד.

10. <u>הארקה</u>

10.1. יש להעביר לחדר התקשורת ולריכוז התקשורת הקומתי קו הארקה מארקת יסוד של המבנה. קו הארקה יהיה 16 ממ״ר לפחות.

10.2. אין למשוך הארקות בין מבנים עבור תקשורת המחשבים.

10.3. את תעלות הרשת יש להאריק לארקת יסוד.

10.4. בכלל חדרי התקשורת תבוצע הארקת ברקים – שתי וערב מעל התקרה האקוסטית, 4 פסי השוואה פוטנציאלים המחוברים שתי וערב ובכבל הארקה בחתך 25 מ״מ. כמו כן, פסי ההשוואה יחוברו ע״י כבל הארקה ללא בידוד תעלות הרשת אשר ימוקמו בחדר, מאחד מפסי ההשוואה יפרסו כבלי הארקה לארונות התקשורת הכבל יהיה בחתך 16 מ״מ.

11. <u>מיזוג אויר</u>

11.1. הזנת חשמל מיזוג אויר.

11.2. בחדר יותקנו 2 יחידות מיזוג אויר מפוצלות אשר הספקם יקבע בהתאם לגודל החלל וכן לכמות הציוד בחדר, המזגנים יעבדו לסירוגין כאשר כל מזגן יהיה בתפוקת קירור בהתאם לפליטת החום של הציוד בחדר התקשורת, במקרה של עליה חריגה בטמפרטורה יש לאפשר עבודה מקבילה של יח׳ המיזוג. במידת הצורך יעמיד הזוכה, יועץ מיזוג בכדי לאפיין את הגדלים והספקי הקירור הנדרשים וזאת בתאום מול הגורמים המקצועיים של משטרת ישראל.

11.3. בלוח חשמל מזגנים תותקן מערכת החלפת מזגנים להפעלה משתנה ע״י שעון שבת ומגענים (יש אפשרות התקנה בלוח הייעודי לחדר תקשורת המחשבים).

11.4. לכל יחידת מיזוג אשר תותקן בחדרי התקשורת יותקן שסתום זינגר. כמו כן, מתחת לכל יחידת מיזוג יותקן מדף נירוסטה הכולל ניקוז למניעת נזילות.

11.5. צנרת הניקוז בחדר תקשורת המחשבים תותקן בנתיב מוגדר שלא יאפשר גרימת נזק לציוד / חומרה במקרה של תקלה בצנרת.

11.6. חיבור למערכת גילוי כיבוי, להפסקת מזגנים בכיבוי בלבד.

12. <u>מערכת החשמל</u>

12.1. בכל חדרי התקשורת נדרש להתקין לוח חשמל ייעודי לחדר התקשורת. לוח החשמל יאושר על ידי משטרת ישראל.

12.2. לוח חשמל חדר תקשורת המחשבים (ייעודי)

12.2.1. הלוח יוזן מהזנת מעגלים חיוניים.

12.2.2. הלוח יוזן מ-2 לוחות חשמל ראשיים (שדה A+ שדה B)

12.2.3. הלוח יתוכנן לקליטת מערכת אל – פסק על פי הנדרש בשטח.

12.2.4. בלוח יותקן מפסק מעקף אל-פסק.

12.2.5. בלוח יותקנו מפסקי הגנות ברקים.

12.2.6. כל מעגל יוגן באמצעות מאמ״ת 16 A .

12.2.7. לכל ארון תקשורת ייפרסו 2 שקעי CEE16A חד פאזי מארון החשמל משדות שונים.

12.2.8. בלוח תותקן מערכת התראה בפני עליית טמפ׳ דיגיטאלית בעלת צג חזותי לחיווי הטמפרטורה. 26 מעלות התראה בזמזם ונורית, כולל התראה מחוץ לחדר מחשב / משל״ט. 32 מעלות ניתוק מערכות חשמל.

12.2.9. סליל הפסקת לניתוק מתחים, בזמן כיבוי בלבד.

12.2.10. בכניסה לחדר מחשב תותקן פטריית הפסקת חירום.

12.2.11. מומלץ להתקין מערכת גילוי רטיבות מתחת ליחידות המיזוג.

12.2.12. בסמכות יועץ התקשורת מטעם המשטרה לקבוע באיזה חדרים ניתן לוותר על הכנת מעגלים יעודיים בלוח החשמל לקליטת יחידות אל פסק.

13. <u>פיזור מכלולי תקשורת (מכלול כולל 4 נקודות מחשבים / טלפוניה)</u>

13.1. בחדר בשטח של עד 7 ממ״ר אשר משמש כמשרד – מכלול 1.

13.2. בחדר בשטח של 7 ממ״ר עד 14 ממ״ר אשר משמש כמשרד - 2 מכלולים.

13.3. בחדר בשטח של 14 ממ״ר עד 18 ממ״ר אשר משמש כמשרד - 3 מכלולים.

13.4. בחדר בשטח של 19 ממ״ר עד 24 ממ״ר אשר משמש כמשרד – 4 מכלולים.

13.5. בחדר ישיבותיותקנו 10 מכלולים (כמות סופית בהתאם לגודל החדר והצרכים המבצעיים)- חלק מהתשתית תהיה תחת הרצפה עבור השולחן המרכזי וזאת בהתאם לדרישות משטרת ישראל.

13.6. בחדרים / משרדים בהם תידרש עמדת מדפסות יש להתקין חצי מכלול בנוסף לעמדות אשר יותקנו בחדר ולפי הגדרת יועץ התקשורת של משטרת ישראל.

13.7. מחסנים, נשקיה, ארכיון – חצי מכלול, או בהתאם לנדרש במכרז.

13.8. שעון נוכחות, שעון הסעדה, רשת WIFI, מערכות בטחון, (אזעקה, גילוי אש) – חצי מכלול – 2 נק׳ תקשורת.

13.9. לכל עמדת הלבנה, מדפסות / פקס יש להתקין מכלול, מיקום עמדות ההדפסה יהיה לפי הגדרת יועץ התקשורת של משטרת ישראל.

13.10. מעבדת סמים : (מיקום וכמויות במפורט באפיון מעבדת הסמים.

13.10.1. עמדת קליטה- 2 מכלולים

13.10.2. עמדת עבודה- מכלול וחצי. (6 נק׳ תקשורת)

13.10.3. אמצעים המתחברים לרשת (משקל, מצלמה וכו׳)- חצי מכלול.

13.11. נקודת מחשב תכלול שני כבלי מחשב מריכוז התקשורת ושקע כפול, או לפי קביעה מדויקת ע״ג תכניות.

13.12. עמדת עבודה תכלול 4 נקודות תקשורת.

13.13. בחדרים מסוימים המוגדרים כחדרים מיוחדים ע״י משטרת ישראל תורחב תשתית התקשורת בהתאם לדרישה.

13.14. פריסת נקודות התקשורת (עמדות/ מכלולי עבודה) תהיה עפ״י העמדת ריהוט פנים, ע״ג תכניות אדריכליות ועל פי המפתחות שצוינו לעיל

14. <u>קישור בין ארונות וריכוזים</u>

14.1. כעיקרון פריסת התשתית תעשה על בסיס התקנים המופיעים בסעיף 16.

14.2. כל ריכוז תקשורת יחובר לריכוז התקשורת הראשי בכבל אופטי 24 סיבים וקישור של 24 כבלי נחושת W8. במידה וקיימים 2 ריכוזי תקשורת ראשיים במבנה יש לחבר כל ריכוז משני בתצורה הרשומה לעיל לכל אחד מחדרי התקשורת הראשיים. גישורי הנחושת יותקנו על פנלים ייעודיים וללא ערבוב עם נקודות קצה.

14.3. בחדר התקשורת הראשי יבוצע גישור מקומי בין ארון השרתים לארון התשתיות/ ציוד אקטיבי ע״ב 24 גישורי נחושת CAT7 וכן גישור אופטי באמצעות סיב MM 24 גידים O.M3. תכנון מפורט יועבר ע״י משטרת ישראל

14.4. כל הסיבים המפורטים יהיו מסוג OM4 \OM3 50 מיקרון ויסתיימו בלוחות ניתוב מתאימים. במידת הצורך יותקנו סיבים משולבים (MM,SM). במידה ויוחלט כי יותקן סיב אופטי מסוג SM העבודה תכלול גם קסטה למגשרים וביצוע ריתוך. כל סיב אשר ייפרס יכלול גם בדיקה במכשיר אלקטרוני. סוג המחבר האופטי אשר יותקן בפנל האופטי יהיה בתצורת LC. תכנון סוג הסיבים יבוצע במהלך האפיון המפורט ולפי החלטת משטרת ישראל

15. <u>אבטחה</u>

15.1. התקנות מערכות התראה וגילוי פריצה בחדר התקשורת יבוצעו בהתאם לדרישות והנחיות חטיבת האבטחה במשטרת ישראל.

15.2. במידה ובחדר יש חלון חיצוני, יש להתקין סורגים וכן גלאי מגנטי ע״ג החלון שיחובר למערכת הכללית.

16. <u>עמדת עבודה בתשתית אחודה</u>

16.1. עמדת עבודה מסוג D-14 תכלול:

* שני שקעי תקשורת כפולים.
* שני שקעי חשמל רגילים (ח״ח).

16.2. D14מולטימדיה

* שני שקעי חשמל רגילים (ח״ח).

16.3. עמדת עבודה מסוג D-18 תכלול:

* שני שקעי תקשורת כפולים.
* ארבע שקעי חשמל רגילים (ח״ח).
* שני שקעי חשמל ממעגל חיוני.

16.4. עמדת עבודה מסוג D-20 תכלול: צינורות לא רלוונטיים

* ארבע שקעי תקשורת כפולים. (4 צינורות 25״)
* שני נק׳ כלבו עבור מולטימדיה (שני צינורות 29״).
* ארבע שקעי חשמל רגילים (ח״ח).
* שני שקעי חשמל ממעגל חיוני.

16.5. כל נקודת קצה תסתיים בקופסת חיבורים כדוגמת גיווס (4 מקומות) או עמדת עבודה משולבת כדוגמת סימה בוקס (לפי הדגמים הרשומים מעלה).

16.6. תכנון סוג עמדת העבודה יבוצע במהלך האפיון המפורט.

17. <u>תקנות ותקנים</u>

כל עבודות מערכות התקשוב יבוצעו על - פי התקנים הבאים:

17.1. ISO 11801 – ת"י 1907 חלק 1, פריסת תשתיות בזק (טלקומוניקציה במבנים מסחריים).

17.2. TIA/EIA569/ – ת"י 1907 חלק 2, פריסת מערכות תיעול והקצאת חללים עבור מערכת תקשורת נתונים.

17.3. GROUNDING & BONDING TIA /EIA – 607.

17.4. ת"י 1907 חלק 3.

17.5. פנלי התקשורת ושקעי הקצה ישאו תקן של CAT6A לפחות, יש להציג אישור של מעבדה מוסמכת.

17.6. כבל התקשורת יהיה מסדרת כבלי GIGA וישא תקן של CAT7 לפחות, יש להציג אישור של מעבדה מוסמכת.

- כבל בודד - 4X2X23/1 S/FTP C7 FR-LSZH RED מק"ט – 9928654103.
- כבל כפול - GIGA-JR 2X(4X2X23#)HFFR F-8 RD מק"ט – 9928692103.

18. <u>תשתית טלפונים – קווי נתונים</u>

18.1. יש להכין תוואי תת"ק מתשתית חברת בזק (מחוץ למתחם) לחדר התקשורת הראשי של משטרת ישראל, התשתית תתבסס על צנרת 4 * 4 צול.

18.2. יש להכין תוואי תת"ק מ- 2 צירים נפרדים של חברת בזק לתוך מבנה התקשורת המשטרתי לצורך שדרוג שרידות מערכות המשטרה.

18.3. על הזוכה להתקין לוח עץ סנדוויץ' בעובי 18 מ"מ מצופה פורמייקה לבנה בחדר המרכזייה.

18.4. מריכוז בזק בחדר התקשורת ייפרס כבל רב זוגי 30*0.5, הכבל יפתח בצידו האחד על גבי פס חיבורים מתנתק (קרונה) ובארון התקשורת קצה הכבל ייפרס על ללוח ניתוב UTP.

18.5. לצורך ביצוע התקנה מושלמת יסופקו האמצעים הבאים: קרונה, אמבטיות לקרונה, פסי סימון וכל הנדרש להתקנה וסידור של הכבילה הרב זוגית.

19. <u>סיכום ודגשים</u>

19.1. הנחיות אלו אינן מהוות תכנון סופי לפרוייקט. התכנון עבור תקשורת המחשבים והטלפוניה יבוצע באופן פרטני בהתאם לצרכים הטכניים שיוגדרו ע"י משטרת ישראל. הנחיות אלו באות לסייע לכל הגורמים בשלבי התכנון הראשונים. בתכנון הקצאת שטחים והבנת הצרכים והדרישות למובילים, לתדרי התקשורת והריכוזים.

19.2. יש לשתף את משטרת ישראל בשלבי התכנון של הפרוגראמה, הקצאת השטחים, תכנון התוואים והנקודות. בכדי למנוע אי הבנות ועל – מנת לקדם את הפרויקט בצורה יעילה.

19.3. באחריות הזוכה להעביר סט תוכניות חשמל תקשורת / אדריכלות / תעלות / תקרה למשטרת ישראל, לצורך העברת הערות ודגשים לפרויקט המתוכנן.

19.4. באחריות הזוכה לבצע את בדיקות התקשורת בזמן, או מיד לאחר מסירת המתקן וזאת בכדי לוודא מסירת אחריות ותקינות של כל אביזרי התקשורת. בכל מקרה דוחות הבדיקה שיופקו יציגו בן היתר את תאריך ביצוע הבדיקה.

19.5. מסירת העבודה תבוצע בצורה מושלמת הכוללת 4 תיקי תיעוד מלאים (AS-MADE), בצירוף כל הבדיקות שנעשו באתר כולל מדיה מגנטית.

19.6. הזוכה יאשר את כלל האביזרים לאישור משטרת ישראל, לפני אספקתו והתקנתו באתר,

19.7. הזוכה מחוייב לבצע את עבודות התקנת תשתית המחשבים / טלפוניה ע"י אחד מקבלני התקשורת, אשר זכו במכרז חשכ"ל.

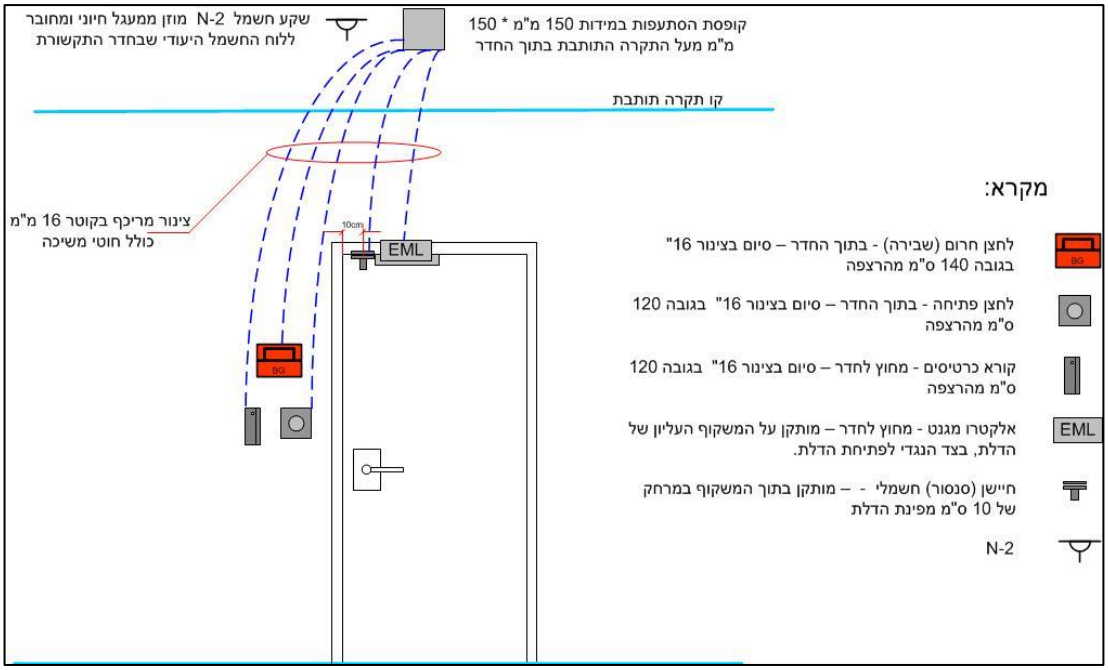
19.8. בכל מקרה הציודים והפריטים אשר יותקנו באתר יהיו על פי הסטנדרט הנהוג באותה תקופה.

19.9. ציוד ההצטיידות כגון: מערכת נעילת חדרי תקשורת, ציוד מולטימדיה, ציוד אקטיבי, שרתים, בנ"מ ועוד ירכשו ע"י משטרת ישראל .

19.10. משטרת ישראל ירכוש ויספק את מערכות האל פסק המיועדות לארונות תקשורת המחשבים בחדרי התקשורת בלבד.

19.11. באחריות הזוכה לקחת בחשבון כי תיתכן סטייה מהתכנון המקורי בגידול כמות המכלולים / נק' התקשורת.

20. <u>מצ"ב שרטוט עקרוני עבור הכנת תשתית למערכת נעילה לחדרי התקשורת.</u>



<u>נספח 5 ב' - דרישות תשתיות</u>

1. **מטרות המסמך**

1.1. לפרט את דרישות משטרת ישראל בנושאי תשתיות לתפעול המרלו"ג ולקשר עם מערכות אחרות של משטרת ישראל.

1.2. תוכנת ה-WMS של המרלו"ג תתמוך בעבודה משולבת מול מערכת ה- ERP של משטרת ישראל (SAP) וכן מערכות מידע ארגוניות נוספות, כאשר בעת העבודה מועברים ומתקבלים נתונים, מידע והזנות חוזרות בין המערכות.

1.3. מובהר בזאת שתוכנת ה-WMS אשר תסופק עבור פרויקט מרלו"ג משטרת ישראל תותקן על תשתיות ייעודיות עבור פעילות משטרת ישראל. תשתיות אלה ימוקמו בחוות השרתים במרלו"ג בהתאם להנחיות ולדרישות משטרת ישראל.

2. **מונחים**

2.1. WMS : warehouse management system – תוכנה לניהול תהליכים ומלאי במחסנים.

2.2. POC : POINT OF CONTACT– איש קשר לפרויקט

2.3. HA : High Availability – זמינות גבוהה

2.4. DB : Data Base – בסיסי נתונים

2.5. DR : Disaster Recovery – התאוששות מאסון

2.6. KPI : Key Performance Indicators – מדדי ביצוע חיוניים

2.7. API : Application Programming Interface – ממשק תכנות יישומים

2.8. Dev : Development Environment - סביבת פיתוח

2.9. Test : Test Environment - סביבת בדיקות

2.10. Pre-Prod : Pre Production Environment - סביבת טרום ייצור

2.11. Prod : production Environment - סביבת ייצור

2.12. RF : Radio Frequency – תדר רדיו

2.13. AP : Access Point - נקודת גישה

2.14. RTO : Recovery Time Objective – זמן מירבי לחזרת מערכת לתפקוד מלא

2.15. RPO : Recovery Point Objective – זמן מירבי לגביו ניתן לאבד מידע

3. **בעלות על המידע**

3.1. כל פעילות הספק הלוגיסטי תנוהל ותאוחסן במערכת המידע הקיימת במרלו"ג עפ"י דרישות משטרת ישראל (שרתים ייעודיים למשטרת ישראל בלבד, DB ייעודי של משטרת ישראל המותקן על שרתים ייעודיים למשטרת ישראל בלבד, ללא משתמשים נוספים וללא שותפים נוספים בתשתיות ובבסיסי הנתונים של משטרת ישראל).

3.2. כלל המידע שיצטבר בשרתים ובבסיסי הנתונים יהיה בבעלות משטרת ישראל בלבד. המידע המתייחס לפעילות הספק עבור משטרת ישראל יהיה זמין בכל עת למשטרת ישראל וללא מגבלה לגבי אופן השימוש במידע.

3.3. מובהר בזאת כי כל המידע הנצבר על שרתי הספק עבור הפעילות של משטרת ישראל הינו חסוי ואינו ניתן לשימוש שאינו במסגרת השירות למשטרת ישראל. כמו כן אין לאפשר נגישות לגורמים שלא אושרו מראש למידע ולתשתיות משטרת ישראל. **אין להעתיק, לשכפל ולגלות את תוכן המידע כולו או חלקו, או למסור מידע לכל גורם שאינו משטרת ישראל ושאינו מאושר על ידי הגורמים הרלוונטיים במשטרת ישראל.**

3.4. מובהר בזאת כי למשטרת ישראל זכות קניין בלעדית על המידע שיצטבר בשרתים.

4. **שיטת העבודה**

4.1. הספק יפעיל מערכת WMS תקנית, כמקובל בשוק. משטרת ישראל שומרת לעצמה את הזכות לדרוש שימוש במערכת WMS לפי שיקול דעתה.

4.2. הספק יתאים (customize) את המערכת עפ"י צרכי משטרת ישראל.

4.3. מערכת ה- WMS של הספק תתממשק למערכות ה- SAP וה "פלא" של משטרת ישראל.

4.4. הספק יטמיע את מערכת המידע (WMS) בכפוף לאפיון שיסוכם מול משטרת ישראל כולל תהליכי בקרה, גיבוי, שרידות, וכלל התהליכים התומכים בתפעול המערכת.

4.5. הספק יהיה אחראי לתפעול, תחזוקה ועדכון שוטף של מערכת ה-WMS.

5. **תחומי אחריות**

5.1. משטרת ישראל תהיה אחראית על מערכות המידע הארגוניות, כדוגמת מערכת ה- SAP וה "פלא".

5.2. משטרת ישראל תהיה אחראית לקליטת המידע שיגיע בממשקים שיוגדרו ממערכת ה- WMS של הספק אל מערכות המידע הארגוניות הנמצאות במשטרת ישראל.

5.3. משטרת ישראל תהיה אחראית לייצא מידע באמצעות ממשקים שיוגדרו אל מערכת ה- WMS של הספק.

5.4. הספק יהיה אחראי על מערכת ה-WMS אשר ברשותו על כלל מרכיביה (תוכנה, תשתית, רישיונות וכו').

5.5. הספק יהיה אחראי להעברה ו/או קליטה של הנתונים באמצעות ממשקים שיוגדרו. תדירות העברה ו/או קליטה תקבע על ידי משטרת ישראל, או על פי אירוע/ים אשר יוגדרו בהתאם לתהליכי העבודה.

5.6. התקשורת תבוצע דרך קו פרטי, כפי שיקבע באפיון המפורט ע"י משטרת ישראל.

6. סביבות עבודה נדרשות

6.1. מערכת ה- WMS לרבות הממשקים תותקן אצל הספק. הספק יפרט את החומרה, התוכנה ותהליך התחזוקה של התוכנה ושל הסביבה בה היא מותקנת (למשטרת ישראל הזכות לדרוש את הסכם השירות עם ספק תוכנת ה-WMS).

6.2. הספק יפרט את ארכיטקטורת מערכת המידע המאופיינת עבור משטרת ישראל. למשטרת ישראל נשמרת הזכות לאשר ו/או לבקש שינויים בארכיטקטורה המוצעת.

6.3. הספק יקים סביבות עבודה מקבילות לסביבת הייצור של המערכת והממשקים:

6.3.1. סביבת DEV עבור פיתוח, שינויים ושיפורים.

6.3.2. סביבת TEST עבור בדיקות המערכת והממשקים. הסביבה תדמה את כלל מרכיבי סביבת הייצור באופן מלא.

6.3.3. סביבת PRE-PROD עבור בדיקות המערכת והממשקים ותאימותה לסביבת הייצור הסביבה תדמה את כלל מרכיבי סביבת הייצור ותהווה תת סביבה בסביבת הייצור.

7. תוכנה

7.1. רשימת התוכנות וסוגי הרישוי שהספק מפעיל:

7.1.1. הספק יפרט את רשימת התוכנות שבכוונתו להפעיל לטובת המערכת. עבור כל תוכנה נדרש אישורה של משטרת ישראל לשימוש בה וזאת לאחר בחינתה על ידי הגורמים הרלוונטיים (אבטחת מידע, סיסטם וכו').

7.1.2. הספק לא יאפשר לעובדיו להתקין במחשבי המרלו"ג תוכנות פרטיות שאינן ממקור בטוח ושנרכשו כדין על ידי הזוכה.

7.1.3. הספק ימנה POC שיעמוד מול משטרת ישראל בנושא תוכנה, אבטחת מידע וסיסטם.

7.1.4. האחריות לרכישת התוכנות והרישוי המתאים הינה על הספק בלבד, כולל תוכנת ה-WMS ותוכנות הסביבות הרלוונטיות.

7.1.5. הספק יציג את תוקף רישיונות התוכנה מעת לעת עפ"י בקשת משטרת ישראל. למען הסר ספק באחריות הספק לדאוג לרישוי תקף לאורך כל הפרויקט וכן לשירותים בעבור שדרוג ועדכוני התוכנות השונות.

7.1.6. הספק יקצה 20 רישיונות למשטרת ישראל לשימוש בו זמנית באתר הספק במערכות המידע בהם הוא עושה שימוש (למשל WMA, POD וכו').

8. תשתיות חומרה ותקשורת

הספק יהיה אחראי על תקינות כלל מערכות התשתית: חומרה ותוכנה במרלו"ג, לרבות הקישור לרשת המקשרת אל משטרת ישראל.

8.1. שרתים ואחסון

8.1.1. הספק יספק מערכי אחסון עפ"י הקריטריונים הבאים:

8.1.1.1. מערך האחסון יהיה בהתאם ליצרני האחסון המובילים בשוק, כדוגמת: HDS, NETAPP, HP.

8.1.1.2. מערך האחסון יהיה מהדור והסדרה העדכניים ביותר של היצרן.

8.1.1.3. מערך האחסון יתמוך בטכנולוגיית HA (High Availability). באחריות הספק ליישם ולהטמיע את תשתית האחסון בתצורת HA.

8.1.1.4. מערך האחסון יהיה ללא SPOF (single point of failure)

8.1.1.5. מערך האחסון יבטיח עבודה רציפה ודינמית בין אתרי הייצור (active-active) , תוך שמירה על רציפות והמשכיות העבודה (ללא נפילה/נתק אפליקטיבי).
באחריות הספק ליישם ולהטמיע את תשתית האחסון בתצורת active-active.

8.1.1.6. מערך האחסון יהיה בעל זמינות מערכת שלא תפחת מרמת זמינות של 99.999% (לא יותר מ-5 דקות השבתה בשנה, תוך הנחת עבודה של עבודה שוטפת 24/7, 365 יום בשנה).

8.1.1.7. מערך האחסון נדרש לספק לאורך כל הפרויקט, יתירות משאבים ונפחים של 35% אל מול משאבי ונפחי צריכת המערכת. למען הסר ספק יתירות זו הינה מעבר ליתירות הנדרשת בהיבטי שרידות וחלוקת עומסים ובהתאם למשאבים הנדרשים לביצועי מערכת מקסימליים.

8.1.1.8. על מערך האחסון לתמוך בדרישות רגולטוריות בהתאם למפורט:

1) immutability (WORM) – בהתאם להגדרות משטרת ישראל
2) versioning – בהתאם להגדרות משטרת ישראל
3) audit trails
4) managed & secure deletion – בהתאם להגדרות משטרת ישראל
5) data privacy and encryption – בהתאם להגדרות משטרת ישראל
6) retention classes – בהתאם להגדרות משטרת ישראל
7) enterprise level compliance (privileged delete, idm api, worm , etc.)

8) data shredding
9) SEC 17a4 compliance
10) FIPS 140-1 complinace
11) encryption aes-256
12) הגנה והבטחת שלמות ומהימנות המידע ומבנה
13) התממשקות מלאה לאימות וזיהוי משתמש מול AD

8.1.1.9. מערך האחסון יאפשר עבודה בפרוטוקול SAN, NFS, CIFS. הספק יפרט את תצורת המערכת תוך פירוט פרוטוקול העבודה.

8.1.1.10. מערך האחסון יתמוך בהוצאת MIB, SNMP. מערך האחסון יתמוך תעבורה מול משתמשים של לפחות 10Gbps (ביתירות ושרידות מלאה).

8.1.1.11. מערך האחסון יהיה ייעודי למשטרת ישראל, ללא משתמשים ושותפים נוספים. למען הסר ספק כלל מערך האחסון יהיה ייעודי, הן ברמת הבקרים והן ברמת הדיסקים.

8.1.1.12. על הספק לציין את נפחי האחסון והביצועים הדרושים עבור המערכת ואת שיעור הגידול השנתי.

8.1.1.13. הספק יציין מהם זמני התגובה הצפויים במערכת לשאילתות ופעולות מסוגים שונים, ומהן ההנחות לגבי עיבוד ותקשורת עבור ביצועים אלה. משטרת ישראל תהא רשאית לבקש הדגמה להוכחת העמידה בזמני התגובה האמורים וכן לבצע בדיקות ביצועים בעצמה.

8.1.1.14. על הספק לתאר האם קיימים פרמטרים המשפיעים על עומסי עיבוד ותקשורת ועל זמני התגובה הצפויים במערכת. במידה וקיימים פרמטרים משפיעים, על הספק לתאר מהם הפרמטרים המשפיעים וכיצד משפיעים.

8.1.1.15. סביבות העבודה השונות יופרדו ברמה לוגית ופיסית באחסון, כך שלא תתאפשר השפעה או קשר כלשהו בין סביבות העבודה השונות אל מול סביבת הייצור.

8.1.2. הספק יספק שרתים עפ"י הפרמטרים הבאים:

8.1.2.1. השרתים יהיו בהתאם ליצרני השרתים המובילים בשוק, כדוגמת: HP, LENOVO, DELL,CISCO וכו'

8.1.2.2. השרתים יהיו מהדור והסדרה העדכניים ביותר של היצרן.

8.1.2.3. השרתים יתמכו בטכנולוגיית HA (High Availability) בכלל רכיביהם, כולל היבטי חיבוריות תקשורתית ודיסקי מערכת הפעלה.

8.1.2.4. השרתים יהיו ללא SPOF (single point of failure).

8.1.2.5. מערך השרתים יבטיח עבודה רציפה ודינמית בין שדרות הייצור (active-active) , תוך שמירה על רציפות והמשכיות העבודה (ללא נפילה/נתק אפליקטיבי).

באחריות הספק ליישם ולהטמיע את מערך השרתים בתצורת active-active.

8.1.2.6. מערך השרתים יהיה בעל זמינות מערכת שלא תפחת מרמת זמינות של 99.999% (לא יותר מ-5 דקות השבתה בשנה, תוך הנחת עבודה של עבודה שוטפת 24/7, 365 יום בשנה).

8.1.2.7. מערך השרתים נדרש לספק לאורך כל הפרויקט, יתירות משאבי זיכרון וכוח עיבוד של 35% אל מול צריכת משאבי זיכרון ועיבוד במערכת ברמת שיא. למען הסר ספק יתירות זו הינה מעבר ליתירות הנדרשת בהיבטי שרידות וחלוקת עומסים ובהתאם למשאבים הנדרשים לביצועי מערכת מקסימליים.

8.1.2.8. מערך השרתים יהיה ייעודי למשטרת ישראל, ללא משתמשים ושותפים נוספים. למען הסר ספק כלל מערך השרתים יהיה ייעודי, הן ברמת שרתים וירטואליים והן ברמת שרתים "מארחים" (HOST).

8.1.3. מערכות הפעלה:

8.1.3.1. הספק ירכוש מערכות הפעלה עדכניות וכן רישוי המאפשר שדרוג המערכות ועדכונן.

8.1.3.2. מערכות הפעלה יהיו העדכניות ביותר בנקודת זמן היישום ויהיו לפחות windows server 2016.

8.1.3.3. מערכות ההפעלה יוקמו בתצורת cluster. הcluster יהיה בגרסה העדכנית ביותר בנקודת זמן היישום ולא יפחת מגרסת ms cluster 2016.

8.1.3.4. מערכות ההפעלה יותקנו בתצורה שתבטיח רציפות והמשכיות העבודה (ללא נפילה/נתק אפליקטיבי).

8.1.4. וירטואליזציה:

8.1.4.1. תשתית הווירטואליזציה תתבסס על vmware בגרסה העדכנית ביותר לנקודת זמן היישום ולא תפחת מגרסה 6.

8.1.4.2. התשתית הווירטואלית תוקם בתצורה בעלת שרידות מקסימלית ובתצורה שתבטיח רציפות והמשכיות העבודה (ללא נפילה/נתק אפליקטיבי).

8.1.4.3. קלסאטר הווירטואליזציה יהיה ייעודי למשטרת ישראל ללא משתמשים ושותפים נוספים.

8.1.5. הספק יפרט את תשתיות החומרה והתוכנה שישמשו את אתר המרלו"ג ויעבירם לאישור משטרת ישראל.

8.2. **איזון עומסים**

8.2.1. הספק יטמיע תשתית המאפשרת איזון עומסים בשרתי המערכת (NLB) תחת מעטפת מוצרים מובילים בשוק, כדוגמת: F5 ו-NETSCALER.

8.2.2. הפתרון יהיה מהדור והסדרה העדכניים ביותר של היצרן.

8.2.3. הפתרון יתמוך בטכנולוגיית HA (High Availability) בכלל רכיביהם, כולל היבטי חיבוריות תקשורתית וספקי כוח.

8.2.4. הפתרון יהיה ללא SPOF (single point of failure).

8.3. **בסיסי נתונים**

8.3.1. הספק ירכוש את בסיסי הנתונים (DB) המקובלים בשוק והמתאימים לדרישות מערכת ה-WMS. לדוגמא: sql, oracle.

8.3.2. בסיסי הנתונים לכלל מערכות המידע/התוכנות יהיו ייעודיים למשטרת ישראל בלבד וללא משתמשים נוספים.

8.3.3. המערכות המשרתות את משטרת ישראל יהיה מערכות עצמאיות וייעודיות וללא תלויות במערכות חיצוניות או מערכות להן שותפים נוספים.

8.3.4. בסיסי הנתונים יותקנו בתצורה שרידה (cluster) המבטיח רציפות והמשכיות עבודה ללא נתק אפליקטיבי.

8.3.5. בסיסי הנתונים יהיו בגרסתם העדכנית ביותר ובהתאם לאישור משטרת ישראל.

8.3.6. הספק יפרט את בסיסי הנתונים שישמשו את המרלו"ג ויעבירם לאישור משטרת ישראל.

8.4. **מערכות שו"ב**

8.4.1. הספק יפרט KPI הנדרשים לניטור המערכת והממשקים השונים ברמת החומרה/תוכנה וכן תהליכים עסקיים במערכת.

8.4.2. הספק יספק שירותי ניטור בהתאם לפרמטרים שיקבעו מול משטרת ישראל ויעבירם למערכת השו"ב המרכזית במשטרת ישראל בהתאם למפורט:

8.4.2.1. ניטור רכיבי תשתית – כלי הניטור לרכיבי תשתית במשטרת ישראל מבוסס על Microsoft SCOM 2012. בחירת הכלי לניטור תבוצע על ידי צוות שו"ב של משטרת ישראל.

8.4.2.2. הגדרת שירותים קריטיים (KPI) – במסגרת מימוש המערכת יוגדרו KPI לניטור שירותים חיוניים. KPI אלה יכללו רכיבי ניטור תשתיתי וכן ניטור אפליקטיבי.

8.4.2.3. הגדרת מדדים כמותיים – במסגרת מימו המערכת יוגדרו מדדים שיציגו בצורה כמותית "ציונים" לעבודה תקינה של שירותים עיקריים של המערכת, בזמן אמת (on-line).

8.4.2.4. ניטור רכיבים אפליקטיביים – במסגרת מימוש הפתרון יבוצע ניתוח של רכיבי היישום ויקבעו רמות סף לניטור תקינות המערכת וכן ממשקיה.

8.4.2.5. המערכת תתמוך בשליחת התרעות בזמן אמת למערכת השו"ב המשטרתית ע"י SNMP או ע"י כלי התרעה נוספים (כדוגמת: web service).

9. **גיבוי, שחזור וזמינות המידע**

באחריות הספק לבצע גיבוי רציף למידע הקיים במערכת לרבות מידע המגיע באמצעות הממשקים.

9.1. **גיבוי**

9.1.1. מערך הגיבוי יוטמע בתצורת HA (High Availability).

9.1.2. מערך הגיבוי יותקן בתצורת active-active כך שתתאפשר רציפות והמשכיות גיבויים גם במקרה של כשל באתר ראשי/משני.ניתן להקים האתר הראשי והמשני באותו תא שטח וע"ב אותם תשתיות.

9.1.3. הגיבויים יבוצעו בתצורת גיבוי לדיסק.

9.1.4. גיבוי יבוצע עבור כל מרכיב מהותי האמור להשפיע על מערכת ה-WMS והממשקים אליה.

9.1.5. גיבוי יבוצע עבור כל המידע במערכת: תצורת שרתים (system state), בסיסי נתונים ומידע מערכת כדוגמת שירותי קבצים וכד'.

9.1.6. הספק יפרט את שיטת הגיבוי, מחזורי הגיבוי, טווח שמירה של כל קבצי הגיבוי וכו'. המידע יישמר בהתאם למדיניות המפורטת:

א) גיבוי יומי מלא – יישמר למינימום 38 יום. עבור כל יום יבוצעו 4 מופעי גיבוי, מדי 6 שעות: 00:00, 06:00, 12:00, 18:00.

ב) גיבוי שבועי מלא - יישמר למינימום 6 שבועות.

ג) גיבוי חודשי מלא – יישמר למינימום 14 חודשים.

ד) גיבוי שנתי מלא – יישמר לעד.

9.1.7. זמינות העתקי גיבוי יהיו בהתאם למדיניות המפורטת:

א) גיבוי יומי – ימצא בזמינות באתר ראשי וכן עותק באתר ה-DR.

ב) גיבוי שבועי – 6 חודשים (24 שבועות) ימצאו באתר ראשי וכן עותק באתר ה-DR.

ג) גיבוי חודשי – 6 חודשים ימצאו בזמינות באתר ראשי וכן עותק באתר ה-DR.

- מעבר לאמור ובהתאם למדיניות המפורטת בסעיף 10.1.6 כלל ההעתקים ימצאו באתר ה-DR.

9.2. **שחזור**

דרישות המינימום לשחזור המידע:

1) ניתן יהיה לשחזר מידע בכל נקודת זמן ובהתאם למועד הרצוי.

2) ניתן יהיה לשחזר מידע ללא תלות במערכת הגיבויים. במידע ותוחלף מערכת הגיבויים ותידרש מיגרציה של המידע המגובה למערכת החדשה, באחריות הספק לבצע מיגרציה זו שתכלול פריסת העתקי הגיבוי כולל תצורת המערכת (שרתים) וביצוע גיבוי מחדש במערכת הגיבוי הרלוונטית לאותה עת.

3) הספק יגדיר תרגולת שחזור שתבוצע אחת לחודש לפחות ותוצאותיה ידווח למשטרת ישראל.

4) הספק יפרט כיצד מתבצעת התמיכה ב-HA למערך השחזורים.
5) הספק ייבצע תרגולות חצי שנתיות לבחינת HA וכן שחזור מ-DR.
6) הספק יתאר ארכיטקטורת מערך השחזור וכן את שיטת השחזור בהתאם לתרחישים שחזורים של המדיניות המפורטת בסעיף 10.1.7.

9.3. **זמינות**

9.3.1. מערכת ה-WMS לרבות הממשקים תהיה זמינה 24/7, 365 יום בשנה, בהתאם ל-SLA שייקבע.

9.4. **רציפות והמשכיות עסקית**

9.4.1. עותקי המידע יאוחסנו באתר נפרד DRבמרחק שלא יפחת מ-60 ק״מ מאתר השרתים הראשי ובהתאם להנחיות משטרת ישראל בהיבט דרישות מבנה (TIER). מיקום האתר יהיה נתון לאישור משטרת ישראל.

9.4.2. האתר ה- DR יכיל **<u>עותקי מידע בלבד</u>** ויעודכן בקבועי זמן שיקבעו אל מול משטרת ישראל בתצורה א-סינכרונית. אתר זה בא להבטיח שמירת העתק מידע עדכני וכן היסטוריה ארגונית, במידה של פגיעת סייבר בתשתית אתר הייצור ו/או ״השחתה״ של המידע בין שדרות ה-active-active של האתר הראשי, עקב כשל כלשהו.

9.4.3. הספק יפרט תרגולים שנתיים לאתר ה-DR (כמות תרגולים, תצורת תרגול, תוצאות תרגול וכו׳).

9.4.4. על הספק לתת מענה לאתר DR מרוחק המקושר בתווך fiber.

9.4.5. כל גידול ו/או שינוי באתר אחד, יהיה מחויב להיות מיושם במקביל באתר המשני.

9.4.6. הספק יפרט את ארכיטקטורת החיבוריות בין האתרים שישמשו את המרלו״ג ויעבירה לאישור משטרת ישראל.

10. **משתמשים והרשאות**

10.1. הספק יפרט את סוגי המשתמשים במערכת ותפקידיהם:
ADMIN, משתמש קצה, מחסנאי, מנהל צוות, מלגזן, מנהל מערכת, בקרים, בקרי ממשקים וכו'.

10.2. ניהול הרשאות: הספק יפרט כיצד יבוצע ניהול המשתמשים והרשאות במערכת.

10.3. AUDIT: הספק יפרט כיצד יבוצע תיעוד וניטור פעולות משתמשי המערכת.
Audit פעולות המשתמשים וכן פעולות במערכת נדרש להישמר למשך 7 שנים.

11. **אבטחת מידע**

על פי נספח אבטחת מידע המפורט במכרז זה

12. **נהלי חירום**

12.1. הספק יכין תוכנית חירום הכוללת טיפול באירועים של תקלות ו/או השבתת המערכת.

12.2. הספק יכין תוכנית חירום הכוללת התמודדות עם כשל באתר ראשי ו/או כשל באתר משני.

12.3. הספק יכין תוכנית חירום הכוללת התאוששות מאסון על בסיס אתר ה-DR.

12.4. הספק יפרט את האופן בו הוא מגבה את המידע ואת הדרך בה הוא משיב את המערכת לפעולה סדירה ותקינה באופן הקצר ביותר, תוך פירוט סדר פעולות והגדרת משכים עבור כל פעולה.

12.5. הספק יפרט:

12.5.1. תכנית השבתה, החזרה לכשירות והתאוששות מאסון.

12.5.2. נהלי חירום, גיבוי מידע וכו'.

12.6. ככלל זמן ההתאוששות מאסון לא יארך מעבר ל-24 שעות.

13. **תיעוד המערכת והדרכות**

13.1. תיעוד – על הספק לכלול את כל התיעוד הנדרש לצורך הקמה מלאה מחדש של המערכת על ידי הלקוח ולצורך תחזוקתה השוטפת והמלאה של המערכת על ידי צוות מיומן מצד הלקוח. על התיעוד לכלול:

13.1.1. תכולת תיק התיעוד.

13.1.2. הסברי מערכות, מודולים ורכיבים.

13.1.3. הסברי זיקות וממשקים במערכת.

13.1.4. ספרות מלאה לכל רכיבי התוכנה.

13.1.5. תיעוד מלא של הממשקים לרבות מסמכי אפיון, בדיקות, התקנות ותפעול.

13.1.6. תיעוד מלא של ההגדרות השונות במערכת.

13.1.7. נהלי תחזוקה, תפעול ופעילות מנע.

13.1.8. פרטי ספקים נותני שירות.

13.1.9. כל חומר עזר נוסף שיידרש לצורך תחזוקה וטיפול במערכת.

13.1.10. דו"ח בדיקות מקיף לתקינות ההתקנה והתפקוד השוטף – צ'ק ליסט.

13.1.11. הדרכות – במסגרת הקמת המערכת, הספק יבצע הדרכה למשתמשי המערכת ומפעיליה.

ככלל על הספק לבצע עדכון התיעוד מדי כל שינוי ו/או עדכון בסביבת העבודה.

13.2. הדרכה –

13.2.1. ההדרכה תכלול:

1) הדרכה בהפעלת המערכות לרמת מפעיל, רמת מטמיע ולרמת מתחזק מערכת.
2) הדרכה באיתור ופתרון תקלות (כולל מתן בנק תקלות ומענים).
3) הדרכה על התיעוד ושיטת העבדה מולו.
4) מדריך למשתמש – עפ"י סוגי המשתמשים.

13.2.2. ההדרכה תתבצע באתר הספק, מתכונת ההדרכה תקבע לפני ביצועה במשותף ע"י הפק ומשטרת ישראל, תוך אישור מנהל הפרויקט מטעם משטרת ישראל.

13.2.3. הספק יעביר למשתתפים תיעוד מלא של ההדרכות והחומר הנלווה, הן בעותק "קשיח" והן ב-soft copy.

14. **שירות ותחזוקה**

14.1. **הגדרות**

14.1.1. **End Of Life (להלן: "EOL")** - הודעה מטעם יצרן, הקובעת זמן או מועד שממנו והלאה לא ייוצר ו/או לא ניתן יהיה להצטייד ו/או לרכוש ציוד או רכיב מסויים (חומרה ו/או תוכנה) של היצרן, שלגביו ניתנה ההודעה.

14.1.2. **End Of Service (להלן: "EOS")** - הודעה מטעם יצרן הקובעת זמן או מועד שממנו והלאה לא יינתנו שירותי תחזוקה ו/או אחריות לציוד או רכיב מסויים (חומרה ו/או תוכנה) של היצרן, שלגביו ניתנה ההודעה.

14.1.3. **"עדכון" (Major/Minor Update)** - תיקון או עדכון של גרסת תוכנה קיימת או חלק ממנה, לרבות תיקון "באגים", שינוי או החלפת ממשקים בתוכנה, Service Pack, תיקון, PATCH, Hot Fix ו/או תיקון אבטחה במוצר, שיפור ביצועים וכיו"ב. עדכון יכול לכלול תיקונים בפונקציונאליות הקיימת ו/או פונקציונאליות חדשה וככל שמטרתה היא לתקן את הליקוי.

14.1.4. **"מועד גילוי התקלה"** – המועד בו התגלתה תקלה במערכת, אם בהודעה טכנית על גבי אחת ממערכות הניהול והבקרה, אם ע"י נציג המשטרה, שנתקל בבעיה תפעולית של המערכת או אם ע"י נציג מטעם הספק.

14.1.5. **"מועד פתיחת תקלה"** – המועד בו העביר נציג מטעם הספק או המשטרה

(הראשון מביניהם) אל מוקד התמיכה של הספק, קריאה ראשונה לטיפול בתקלה.

14.1.6. **"זמן לתחילת טיפול ממועד פתיחת התקלה"** - המועד שיחל מרגע מועד פתיחת התקלה במוקד הספק ועד לרגע בו החלה הספק לטפל בתקלה על ידי הגורם הרלוונטי.

14.1.7. **"מועד מתן תרופה (Work Arround)"** - המועד בו הצליח הספק, להנחת דעתה של המשטרה, להתגבר על החלק העיקרי של התקלה, להפעיל את מירב הפונקציות ולהשמיש את עיקר יכולותיה של המערכת שבאחריותה, כל זאת מבלי שהמערכת חזרה לפעילות מלאה, על כל מרכיביה (חומרה ותוכנה).

14.1.8. **"מועד סיום טיפול בתקלה"** - המועד בו הכריז הספק כי המערכת חזרה לפעילות מלאה, על כל מרכיביה (חומרה ותוכנה).

14.1.9. **"מועד סגירת תקלה"** – המועד בו אישרה המשטרה, כי המערכת מתפקדת בתקינות טכנולוגית ויישומית, על כל מרכיביה (חומרה ותוכנה).

14.1.10. **זמן השבתה (Down Time)** - הזמן המצטבר של כל תקלה בפני עצמה, החל ממועד פתיחת תקלה (לספק), ועד מועד סיום טיפול בתקלה או מתן תרופה – המוקדם מביניהם.

14.1.11. **"משך השבתה לתקלה"** - הזמן המצטבר של כל תקלה בפני עצמה, החל ממועד פתיחת תקלה (אצל הספק), ועד מועד סגירת התקלה, למעט עיכובים הנגרמים על ידי המשטרה.

14.1.12. **"יעד השבתה שנתי"** – הזמן השנתי המצטבר של המערכת וכולל זמני ההשבתות בין אם בגין תקלות או לאו (ממוינות ע"פ דרגת חומרתן בהסכם), המשמש למדידת עמידות המערכת – מחד, ועמידת הספק – מאידך, במדדי העמידה בנספח התחזוקה בין הצדדים.

14.1.13. **חלון שירות** - כל ימות השנה, במהלך כל שעות היממה ובתאום עם המשרד ועם המשטרה, כולל חגים ומועדים 24/7/365.

14.1.14. **סיווג תקלות**:

14.1.14.1. **"תקלה קריטית"-** תקלה שתוצאותיה הינה אחת ו/או יותר מבין המפורט להלן:

א) השבתת המערכת המרכזית.

ב) תקלה אחת או מספר תקלות אשר צירופן יחד ו/או כל אחת מהן עלולה לגרום להשבתת המערכת.

ג) תקלה העלולה לגרום לאובדן מידע, כגון אי קליטת מידע או אגירתו.

ד) תקלה בגישה למאגרי המידע של המערכת, בין אם בהפעלת ממשק המשתמש ובין בממשקים או גישה למערכת.

ה) תקלה העלולה לגרום לשיבוש של נתונים במערכת.

ו) תקלה הגורמת לפגיעה פונקציונאלית בתוכנה או בחומרה .

ז) תקלת במ״מ - פירצה אבטחתית ו/או כל תקלת במ״מ, בהתאם להחלטת המשטרה.

14.1.14.2. **״תקלה חמורה״** –תקלה שתוצאותיה הינה אחת ו/או יותר מבין המפורט להלן :

א) כל תקלה העלולה להתפתח לקריטית.

ב) תקלה אחת או מספר תקלות אשר צירופן יחד ו/או כל אחת מהן, עלול לפגוע בפונקציונאליות המערכת כולה, או מודול שלם בתוכה.

ג) ירידה של למעלה מ- 25% בביצועי המערכת, ו/או ביכולת וקיבולת המערכת.

ד) תקלה בממשק המשתמש אשר אינה גורמת לאיבוד מידע, אך מונעת גישה אל חלק מן המידע.

ה) תקלה בביצוע גיבויים.

ו) תקלה בעדכון אחת ממערכות הבמ״מ.

ז) תקלה בהעברת מידע ו/או ממשקי המערכת מול מערכות השו״ב הארגוניות.

ח) אי קבלת התראות מהמערכת.

ט) אי יכולת גישה תחזוקתית למערכת.

14.1.14.3. **״תקלה בינונית״** - תקלה שתוצאותיה הינה אחת ו/או יותר מבין המפורט להלן :

א) תקלה שאיננה משביתה את המערכת או חלקים ממנו.

ב) ירידה של-25% ומטה בביצועי המערכת.

ג) יכולת פונקציונאלית לא תקינה.

14.1.14.4. **״תקלה קלה״** - כל תקלה שלא הוגדרה לעיל, או כל תקלה שאינה משפיעה ישירות על ביצועי המערכת ו/או תקינות קבלת תוצרים.

14.1.14.5. **״תקלה חוזרת״** - כל תקלה אשר חוזרת באותו מכלול או חלק מהמערכת לאחר פחות משבועיים מסיום הטיפול בה תחשב כתקלה חוזרת.

15. <u>שירות ותחזוקה</u>

15.1.1. הספק יתחייב למתן תחזוקה ושירות למערכות המסופקות על ידו ממעוד העלייה לאוויר ולמשך כל תקופת ההסכם.

15.1.2. בתקופת ההסכם יהיה הספק אחראי לתקינות המערכת והממשקים ולמתן התמיכה למערכת והממשקים. באחריות הספק לתקן את המערכת באם התקלקלה או נמצאה לא תקינה בתקופה זו, בהתאם ל-SLA שיפורט בנספח זה.

15.1.3. במסגרת תקופת ההסכם על הספק להתקין עדכוני גרסאות בהתאם לאישור שיינתן ממשטרת ישראל. באחריות הספק ליידע את משטרת ישראל לגבי כל עדכון גרסה (מינורי או ראשי) שיצא תוך שבועיים מיציאתו ולתאם אל מול משטרת ישראל את השיטה וזמן העדכון.

15.1.4. בשנה הראשונה או עד גמר העלייה לאוויר, תהיה משטרת ישראל רשאית להזמין מהספק שינויים, תוספות ושיפורים למערכת, אם וככל שיידרש למשטרת ישראל, ללא כל תשלום ו/או תמורה נוספת לספק ובהתאם ללוחות הזמנים אשר יסוכמו עם הספק במהלך ההסכם.

15.1.5. הספק מתחייב לספק תחזוקה שוטפת למערכת ה-WMS.

15.1.6. הספק מתחייב למתן תשובות לשאלות ובעיות באמצעות הטלפון לכלל הגורמים המקצועיים המעורבים בהפעלת המערכת.

15.1.7. הספק אחראי לדאוג לפעילות תקינה של המערכת, בהתאם למסמך הדרישות הטכני, וזאת במשך כל תקופת הפרויקט, לרבות בתקופת האחריות ובתקופת התחזוקה. לצורך כך יקים הספק צוות תפעול ותחזוקה, שיפעל בשיתוף פעולה מלא עם המשטרה.

15.1.8. הספק מתחייב לספק מענה מקצועי, לכל סוגיה ו/או בעיה ו/או ליקוי ו/או דרישה הנוגעת לתפקוד המערכת, באמצעות הצוות התפעולי האמור, לרבות באמצעות מומחים או יועצים חיצוניים מהארץ או מחו"ל, ככל שהדבר יידרש ובכפוף לאישור המשטרה.

15.1.9. במסגרת תקופת ההסכם על הספק לתעד את כל הפניות והתקלות ביומן תקלות. משטרת ישראל תקבל דו"ח רבעוני מסכם לכלל התקלות ופניות השירות במערכת. התיעוד יכלול מהות הפניה/תקלה, תיאור הפעולה שנעשתה, סיכום כל פעילות שבוצעה, פירוט הרכיבים חומרה/תוכנה, זמן הביצוע ומשכו וכן הגורמים המבצעים.

15.1.10. הספק ידווח באופן שוטף למשטרה, על תקלות ו/או פעילויות, אשר דורשות השבתה חלקית ו/או מלאה של המערכת, עקב דרישות התחזוקה וכל זאת בתאום מלא מול צרכי המשטרה, ומבלי לפגוע ביעדי הזמינות.

15.1.11. שירות התחזוקה יכלול, בין היתר, תפעול ו/או דיווח על תקלות, טיפול בתקלות, מעקב אחר תקלות, עדכון ומסירת מפרטים ו/או שרטוטים ועדכוני מערכת ובדיקתם.

15.1.12. הספק תפרט כיצד בכוונתה לממש את מחויבויותיה על פי נספח זה, כדוגמת אספקת חלקי חילוף בעת תקלות, צוות תמיכה בישראל.

15.1.13. הספק תעשה שימוש בכלי לניהול תצורה עבור כל גרסה ועדכון במערכת. הספק תפרט את הכלי בו ייעשה שימוש.

15.2. שיטת השירות והתחזוקה

15.2.1. במידה ואירעה תקלה, הספק יהיה אחראי לאיתור מקור התקלה, לתקן ו/או להחליף על חשבונו על פי לוחות הזמנים ושאר התנאים המפורטים בנספח זה ו/או בהוראות יצרן, כל פריט או מכלול חומרה ו/או תוכנה במערכת (או את כל המערכת) וכל פגם גלוי או נסתר, שהתקלקל או שאינו עומד בדרישות הביצועים הקבועים במסמך הדרישות הטכני, ככל שיתגלה בעתיד בפעולת המערכת, וזאת עד לפעילות תקינה של המערכת.

15.2.2. הספק אחראי לניהול ממוכן של הקריאות אשר נתגלו במערכת, באמצעות מערכת לניהול תקלות. מערכת ניהול התקלות תמוקם באתר הספק ובה ינוהלו התקלות.

15.2.3. הספק יציג ויפרט את מערכת ניהול הקריאות המוצעת על ידו ואת הבנתו את תהליך הטיפול בקריאות ובתקלות .

15.2.4. הספק אחראי על כלל הקריאות, גם אם הועברו על ידו לטיפולו של צד ג'. העברת קריאה לטיפול צד ג', לא תגרע ממחויבות הספק לעמידה ב- SLA כאמור בנספח זה.

15.2.5. הספק מתחייב כי תיקון תקלה ו/או פגם ו/או קלקול אשר יתגלה במערכת, יתוקן ברציפות וללא הפסקה בהתאם ל SLA וסיווג התקלה, עד השלמת התיקון מבלי שהדבר יזכה את הספק בתמורה נוספת כלשהי.

15.2.6. כל מרכיב חומרה או תוכנה (מכלול או רכיב בודד) שנתגלתה בו תקלה משביתה או
מאיטה, יוחלף פיזית ע"י הספק במרכיב חדש זהה או טוב יותר וללא תוספת עלות, הכל מבלי לפגוע ביעדי הזמינות המפורטים בנספח זה, בתאום עם מנהל הפרויקט ואישור מראש של נציג משטרת ישראל.

15.2.7. פריטים פגומים ו/או תקולים בצורה חלקית או מלאה ואשר יוחלט על החלפתם, יבוצע להם נוהל "השחרה" כמפורט בנהלי אבטחת המידע המשטרתיים. רכיבים אוגרי מידע, כדוגמת דיסקים, יועברו באופן ידני על ידי נציג הספק לידי המשטרה. רכיבים אלו יעברו גריסה מבוקרת בתוך אתר המשטרה כמפורט בנספח במ"מ.

16. <u>עדכונים</u>

16.1. עדכונים למערכת

16.1.1. שירותי התחזוקה כוללים עדכונים, תיקונים ו/או התאמות של המערכת, עדכוני תוכנה למערכות ההפעלה, לאפליקציות ו/או כל רכיב תוכנה אחר, זאת, כחלק מנספח זה, בין הספק למשטרה, ללא כל תמורה נוספת.

16.1.2. הספק מתחייב להתקין כחלק משירות התחזוקה הנ"ל, עדכוני תוכנה מעת לעת, עפ"י המלצת היצרן.

16.1.3. עדכונים אשר עשויים להשפיע על תקינות או טיב מענה המערכת ו/או תפקודה, לא ימומשו על ידי הספק, כל עוד לא ניתן אישור בכתב על ידי המשטרה וכל עוד לא הודיעה המשטרה כי היא ערוכה למימוש השינוי.

16.1.4. למשטרה בלבד שמורה הזכות לוותר על עדכון יחיד או על מספר עדכונים, אם וויתור מלא ואם חלקי, זאת בהודעה כתובה מראש לחברה ובתיאום בין הצדדים. גם אם ויתרה המשטרה על עדכון יחיד או מס׳ עדכונים, הספק ימשיך לתחזק את המערכת באותם תנאים ככל הניתן ביחס לאפשרות העדכון המוצע על ידי הספק.

16.2. תחזוקת תוכנות תשתית ומערכות הפעלה :

16.2.1. ככלל, כל תוכנות התשתית אשר יותקנו בפרויקט יהיו בגרסאות העדכניות ביותר, שהינן בתוקף ומתוחזקות בצורה שוטפת ע״י הספק ובהתאם להוראות היצרן.

16.3. עדכוני תוכנות תשתית ומערכות הפעלה:

16.3.1. כל עדכון לא ימומש על ידי הספק, כל עוד לא ניתן אישור בכתב על ידי המשטרה וכל עוד לא הודיעה המשטרה כי ערוכה למימוש השינוי.

16.3.2. הספק יתקין עדכון תוכנת תשתית לפחות פעם בשנה, לכל אחת מתוכנות התשתית, בהנחה ופורסם עדכון והמשטרה החליטה לבצע את העדכון בתוכנת התשתית.

16.3.3. הספק מתחייב להתאים את המערכת לגרסה המעודכנת של תוכנות התשתית, תוך פרק זמן של עד 90 ימי עבודה מיום קבלת ההתראה מהמשטרה.

16.3.4. לעניין תוכנות התשתית, נכללים גם עדכונים של מערכות הפעלה בתחנות הקצה של המערכת והשו״ב.

17. <u>EOL או EOS של המערכת או רכיביה</u>

17.1. בכל מקרה בו ייוודע לספק ו/או בכל מקרה בו הוא סבור כי אחד מהיצרנים של מרכיבי המערכת, הכריז או בכוונתו להכריז, על חלק ו/או רכיב כלשהו ממרכיבי המערכת, כ״תום ייצור״ ו/או ״תום שירות״ (EOL, EOS) (להלן: ״**ההודעה**״) ויש בהודעה כדי להשפיע בדרך כלשהי על המערכת ויכולותיה, יודיע על כך הספק למשטרה מיד עם ידיעת הדבר.

17.2. עם קבלת ההודעה, יתאמו הצדדים את האופן בו יבוצע החלפת החלק/רכיב במערכת, מבלי שיהיה בכך כדי לפגוע בפעילות תקינה של המערכת ו/או במערכות המשטרה.

17.3. הספק יהיה אחראי על נקיטת כל הפעולות והצעדים הדרושים למימוש וביצוע החלפת הרכיב על חשבונו.

18. <u>תחזוקת חומרה</u>

18.1. במהלך תקופת האחריות ותקופת התחזוקה, יוחלף פריט תקול בפריט מקורי, חדש וזהה או בעל מפרט טכני, שאינו נופל מן הרכיב המקורי, ללא תמורה נוספת. הרכיב המחליף יאושר מראש ובכתב ע״י המשטרה, וכל פעולה הנדרשת לשם הכנסתו, תבוצע ע״י הספק, ללא כל תמורה נוספת ובכפוף לזמני התגובה לטיפול בתקלות, המפורטים בהמשך.

18.2. החלפת רכיב תקול ברכיב חדש, תיעשה ללא החזרת הרכיב התקול, בכפוף לנוהל NRP (Non-Returnable Parts) הבא:

18.2.1. אמצעי אחסון נתונים שהתגלתה בו תקלה, יתוקן באתרי המשטרה ו/או המרלו״ג ו/ ולא ייצא את אתרי המשטרה ו/או המרלו״ג.

18.2.2. ציוד המכיל אמצעי אחסון נתונים, שנתגלתה בו תקלה שלא ניתן לתקנה באתרי המשטרה ו/או המרלו"ג ואין ברירה אחרת אלא לקחתו לצורך תיקון, יוצא מתחום אתרי המשטרה ו/או המרלו"ג, רק לאחר שיישלף מתוכו אמצעי אחסון הנתונים. אמצעי אחסון הנתונים יותקן חזרה בציוד לאחר שזה יוחזר למשטרה ו/או למרלו"ג מתיקון. פירוק והרכבת אמצעי האחסון ע"י הספק, ללא כל תמורה נוספת ובכפוף לזמני התגובה לטיפול בתקלות, המפורטים בהמשך.

18.2.3. אמצעי אחסון נתונים שלא ניתן לתיקון, יוחלף באמצעי אחר בעל מפרט טכני שאינו נופל מן הרכיב המקורי.

18.2.4. אמצעי אחסון נתונים מקולקל שהכיל נתונים ואין להוציאו מרשות המשטרה ו/או המרלו"ג, לא יוחזר לחברה כנגד הרכיב החדש, אלא יועבר לרשות המשטרה.

18.2.5. הקביעה איזה חלק מן הציוד הוא אמצעי אחסון נתונה היא למשטרה ובהתאם לשיקול דעתה הבלעדי. קביעה בנושא זה היא סופית אף אם משמעותה היא שאין להוציא ציוד מאתרי המשטרה ו/או המרלו"ג.

18.3. הספק מתחייב כי כלל רכיבי החומרה שיסופקו על ידו במסגרת ביצוע הפרויקט, יהיו רכיבים אשר לא יקבע ביחס אליהם על ידי היצרן EOL/EOS בטווח של 3 שנים ממועד אישור משטרת ישראל למבצעיות המערכת.

18.4. **<u>במידה ויוכרז EOL/EOS על ידי היצרן לפני התקופה האמורה</u>**, יהיה הספק אחראי להחליף על חשבונו, את הרכיבים האמורים, להתקינם, לוודא את תקינות ותאימות התוכנות הרלוונטיות לאותם רכיבי חומרה ולוודא את פעילותה התקינה של המערכת, ולספק שרותי תחזוקה, בהתאם למסמך הדרישות הטכני ונספח זה.

18.5. **<u>במידה ויוכרז EOL/EOS על ידי היצרן לאחר התקופה האמורה</u>**, המשטרה תישא בעלות הרכיבים האמורים, בהתאם לשיקול דעת המשטרה ו/או במידה ותהא בהם תקלה שאינה ניתנת לתיקון. במקרה כזה, יהיה הספק אחראי, על חשבונו, להתקין את הרכיבים החדשים, לוודא את תקינות ותאימות התוכנות הרלוונטיות לאותם רכיבי חומרה ולוודא את פעילותה התקינה של המערכת בהתאם למסמך הדרישות הטכני ולספק שרותי תחזוקה, בהתאם להוראות נספח זה.

18.6. הספק מתחייב כי במקרה שבו תיפסק פעילותו של יצרן החומרה מכל סיבה שהיא, יתאים הספק את המערכת <u>על חשבונו</u> לחומרה חליפית (לרבות התאמת החומרה והתוכנה, בדיקות לעמידה בדרישות מסמך הדרישות הטכני). התקנת החומרה החליפית תבוצע על ידי הספק, ללא עלות, בעוד רכש החומרה החליפית יבוצע על חשבון המשטרה ובהתאם לשיקול דעת המשטרה. במקרה כזה יהיה הספק אחראי לתחזוקת החומרה החליפית בהתאם להוראות נספח זה.

19. <u>בדיקות</u>

19.1. כל גרסה חדשה של מערכת הפעלה, אפליקציה, יישום או מוצר צד ג', תיקון וכיו"ב, העשויים להשפיע על תפקוד המערכת, יעברו ניסויי מעבדה בסביבת פיתוח שבאתר הספק ולאחר מכן בסביבת הטסט. לאחר מכן, הספק יהיה אחראי להציג את תקינות הגרסה לטובת התקנה בסביבת הפרה-פרוד בטרם העלאתה לייצור.

19.2. הספק יעביר למשטרה בקשה מראש לאישור מועד ביצוע בדיקות.

19.3. בסיום הבדיקה, תיערך פגישה עם המשטרה, בה יציג הספק את תהליכי הניסוי והתוצאות וכן את תוצאות הסימולציה לבדיקת ביצועים ועומסים, בהתאם למוגדר במסמך הדרישות הטכני. כל אלו יהוו מצע להחלטת המשטרה על התהליך הנדרש לאישור העדכון/שדרוג. עם זאת, אי תאימות של גרסה חדשה בעת שחרורה הראשון, אינו תנאי מספיק לא לספקה למשטרה מאוחר יותר. הספק מתחייבת מראש כי יבצע את כל ההסבות וההתאמות הנדרשות למרכיבי המערכת הקיימים – בעת הכרזת כל גרסה וגרסה, כך שיפעלו בצורה תקינה בפרויקט.

20. <u>בדיקות תקינות ותחזוקה מונעת</u>

20.1. בדיקות תקינות ואחזקה מונעת למערכת, תבוצענה ע״י הספק.

20.2. הספק יגיש לאישור המשטרה עד לתחילת בדיקות SAT, נוהל המפרט את תכולת תחזוקת שבר והאחזקה המונעת הנדרשות ואת תדירות האחזקה המונעת (לכל הפחות, אחת לחצי שנה) וכן תוכנית בדיקות שנתית.

20.3. במהלך תקופות האחריות והתחזוקה, כלל פעולות האחזקה שבר/מונעת למערכת ושדרוגי תוכנה, יבוצעו ע״י הספק, בתיאום משטרת ישראל.

20.4. הספק מתחייב לבצע טיפול מונע ובדיקות תקופתיות כפי שהדבר נדרש לעמידה בפונקציונאליות המערכת, לפי הוראות יצרן ותנאי מסמך הדרישות הטכני, כל זאת מבלי לפגוע ביעדי הזמינות המפורטים בנספח זה.

20.5. במסגרת טיפולים מונעים נמנים טיפולים תקופתיים כגון: מעקב אחר ביצועי המערכת וכוונונה, בדיקת עמידה ב-SLA המפורט בנספח זה, מעקב לוגים, כיוונון מסד הנתונים, אינדקסים, הקצאת שטחים, ניקוי שטחים, ניהול עבודת המערכת מול מערכות וממשקים חיצוניים, עדכוני חומרה, תוכנה, קושחה וכו׳. בנוסף, מעקב אחר תפקוד החומרה, צריכת CPU, זיכרון, רה-ארגון דיסקים, תכניות גיבוי ושחזור, מעקב אחר הודעות במערכת השו״ב וטיפול בהן וכיו״ב.

20.6. מועד לביצוע התחזוקה המונעת יתואם עם המשטרה מראש ועד לא יאוחר משבועיים ממועד עריכתן. בדיקות יתבצעו גם אם לא נתגלו בעיות במערכת, במהלך חצי השנה, מאז הבדיקה הקודמת.

20.7. במסגרת בדיקות התקינות והתחזוקה המונעת נכללים גם פעולות הגיבוי והשחזור השוטפות, ביצוע בדיקות ותרגילי השבתת מערכים והפעלת הגיבויים המתאימים, בהתאם למפורט בסעיף הגיבויים.

20.8. בכל מקרה של השבתה יזומה, הספק נדרש לקבל את אישור המשטרה ולתאם לפחות 10 ימי עבודה מראש. המשטרה יכולה לדחות את מועד ההשבתה היזומה, בהתאם לשיקול דעתה הבלעדי, ובתיאום עם הספק.

20.9. עבודות תחזוקה מונעת לא יגרמו להשבתה של המערכת .

20.10. זמן כולל של השבתה יזומה לרכיבים המטופלים, מוגבל ל-4 שעות במצטבר ברבעון, בשעות הערב והלילה או בשעות שיקבעו ע״י המשטרה.

20.11. הספק יגיש למשטרה דו״ח המסכם את הבדיקות בתחזוקה המונעת. פורמט הדו״ח ומועדי

הגשתו יתואמו בין הצדדים.

21. יעדי זמינות ודיווח אירועים - SLA

21.1. הספק מתחייב לספק בתקופת האחריות ובתקופת התחזוקה, ככל שתמומש, שירות ברמה הקבועה ב- SLA.

21.2. המשטרה תהיה זו שתגדיר לחברה את סוג התקלה וחומרתה בהתאם לשיקול דעתה הבלעדי.

21.3. סוגי התקלות, זמן השמשה ע"י פתרון זמני (work around) וזמן עד לפתרון התקלה, כמפורט להלן:

סוג תקלה	זמן לתחילת טיפול ממועד פתיחת התקלה	יעד השבתה עד למתן פתרון זמני (Work Around)	מתן פתרון מלא (עד לסגירת התקלה)
קריטית- emergency	30 דקות	2 שעות	4 שעות
חמורה – major	1 שעה	4 שעות	8 שעות
בינונית - medium	2 שעות	12 שעות	24 שעות
קלה – minor	תחילת יום העבודה הבא	3 ימי עבודה	10 ימי עבודה

21.4. תקלות קריטיות וחמורות יטופלו ברציפות ומסביב לשעון (7X24X365, לרבות ערבי חג, חגים ומועדים), עד לסיום הטיפול בתקלה בהתאם ליעדי הזמינות המפורטים בנספח זה.

21.5. תקלה חוזרת תטופל באופן הבא: סיווג התקלה יעלה רמה אחת. לדוגמא - תקלה בינונית תהפוך לחמורה ותקלה חמורה תהפוך לקריטית. הספק יטפל בתקלה על פי הקריטריונים של הסיווג החדש.

21.6. זמני השבתות אשר באחריות המשטרה, לא יכללו בחישוב זמן ההשבתה, כהגדרתו בנספח זה.

21.7. לא יחשב פרקי זמן בהם מבוצעת פעילות תחזוקה מונעת בפרויקט, ככל שתואם הדבר מראש עם המשטרה.

21.8. הספק ינהל רשימת בעלי מקצוע שתומכים במערכת. למשטרת ישראל הזכות לבקש את הרשימה ולדרוש להחליף את נותני השירות מעת לעת.

נספח 5 ג' - דרישות אבטחת מידע (M,S)

1. כללי

1.1. אבטחת מידע מוגדרת כמכלול הפעולות והאמצעים הננקטים והמיושמים בפרויקט על מנת להגן מפני פגיעה בחסיון, שלמות, אמינות וזמינות המידע. בסעיף זה מתוארות הדרישות ליישום אבטחת מידע במערכת.

2. אבטחת מידע - מושגים

2.1. **שמירת סודיות – Confidentiality**

2.1.1. מידור: מניעת חשיפת מידע של משטרת ישראל בפני כל גורמי צד שלישי המעורבים בתהליך הלוגיסטי .

2.1.2. זליגת מידע: מניעת חשיפה של המידע לגורם חיצוני שלא קשור לתהליך הלוגיסטי ומניעת חשיפת המידע לגורם עוין.

2.2. **אמינות המידע - Integrity**

2.2.1. מניעת שיבוש: שינוי המידע המקורי, הבטחת אי שיבוש המידע המקורי כפי שעבר במערכת, תוך שמירת אמינות מקוריותו עפ"י החוק.

2.3. **זמינות המידע - Availability**

2.3.1. מניעת שירות- DOS/DDOS: מניעת הפלת מערכת המידע של הזוכה וגרימת הפסקת שירות כתוצאה מכך.

2.3.2. הבטחת רציפות השירות: יצירת יתירות (Redundancy) של המערכות, גיבוי המידע ושמירתו באתר מרוחק, שימוש באתר חירום ונהלי הבטחת רציפות השירות – DRP.

3. הגדרת מערכות וממשקים מחשוביים

3.1. מערכות המציע/הזוכה – כלל האמצעים המחשוביים לרבות שרתים, תחנות, אפליקציות, אמצעי תקשורת וכד' שהזוכה מספק ומתפעל במתקן שיבחר.

3.2. ממשקי העבודה המחשוביים בין מערכות הזוכה למערכות המשטרה – מגדירה ומתארת את סוג וצורת העברת הקבצים/מסרים ממערכות המשטרה אל מערכות הזוכה ולהיפך.

3.3. ציוד מחשוב של המשטרה באתר הזוכה – תחנות עבודה מרוחקות וציוד נלווה המחוברים לרשת המשטרתית או רשת אחרת עבור יחידת הפיקוח.

4. אמצעי אבטחת מידע (במ"מ)

4.1. מערכות הזוכה תהיינה מאובטחות באמצעות טכנולוגיות ואמצעי אבטחת מידע המקובלים בשוק על מנת להבטיח רמת אבטחת מידע גבוהה, כמקובל במגזר העסקי לאבטחת מערכות אלו ואשר יאושרו כמספקות ע"י מחלקת אבטחת מידע של משטרת ישראל.

4.2. הזוכה יממש מידור קפדני, שימנע חשיפה של נתוני משטרת ישראל, ונתוני ספק אחד לספק אחר או לכל צד אחר המעורב בתהליך הלוגיסטי.

4.3. הזוכה ישלב במערכת אמצעים המקובלים בשוק למניעת התקפות על מערכותיו, כמפורט בסעיפים להלן.

4.4. המציע יציין את שמו של המנהל או האחראי מטעמו על אבטחת מידע בארגון, הכשרתו והסמכותיו, ויפרט את פרטי הקשר שלו.

4.5. המציע ינהל תהליך מודעות עובדיו באתר לאבטחת מידע והשלכותיה. יש לצרף תיעוד של יישום תהליך זה אצל המציע.

5. קישוריות

5.1. כל הקישוריות בין רשת מערכת הספק המציע לרשת משטרת ישראל תהיה באמצעות העברת קבצים על תשתית כספות של המשטרה באמצעות בודל ותשתית CyberArk.

5.2. הזוכה ישלח ויקבל קבצים באמצעות תוכנת לקוח CyberArk מול שרת כספות .

5.3. לא תהיה תקשורת ישירה כלשהיא בין רשת הזוכה לרשת המשטרה.

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

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

6. אבטחת תשתיות תקשורת

6.1. הזוכה יתקין את מערכות המוצעות ברשת מופרד מכל מערכת אחרת שלו במתקן שיבחר.

6.2. הסגמנטציה המוצעת תכלול הפרדה מיטבית מאיומי רשת האינטרנט, ותבטיח צמצום האיומים למול משטרת ישראל וספקיה.

6.3. הזוכה יתקין, יתפעל ויעדכן מערכות אבטחת תשתיות ותקשורת מקובלות בענף, אשר יכללו לכל הפחות :

6.3.1. חומת אש – FireWall

6.3.2. מערכת למניעת חדירות - IPS

6.3.3. אנטי וירוס ומניעת תוכנה זדונית - Anti-Virus

6.4. הזוכה יגדיר חוקים אשר ימנעו חדירה למערכת, ויבקר באופן שוטף את יעילות החוקים באבטחת המערכת.

6.5. באם במערכת הזוכה יהיה שימוש במסופונים ותקשורת אלחוטית מסוג WIFI, התקשורת בין המסופונים לשרת/תחנת עבודה תהיה מוצפנת ברמת הצפנה המקובלת בשוק של WPA2 לפחות. המציע יפרט את מנגנוני ההצפנה המיושמים במערכת.

6.6. באם התקשורת הנה מסוג אחר (לא WIFI), יפרט המציע את מנגנוני ההצפנה והאבטחה המיושמים במערכת.

6.7. באם נדרשת תמיכה מרחוק למערכת הזוכה לצורך טיפול בתקלות, הדבר יבוצע בצורה מאובטחת ע"י הקמת VPN בין גורם התמיכה מול מערכת הזוכה באתר המקומי,

ההזדהות תהיה אישית וב- FW יבוצעו הגדרות מתאימות לגישה רק לתומכים שיוגדרו מראש.

6.8. הזוכה יתאים את אמצעי אבטחת המידע לאיומים, כפי שיוגדרו ע"י הזוכה במשותף עם משטרת ישראל מעת לעת.

6.9. הזוכה ירשום כל פעילות במערכות התקשורת ורכיבי אבטחת המידע באמצעות יומן פעולות (Audit Log) ויבקר אותו כמוגדר בסעיף המתאים במסמך זה.

6.10. למען הסר ספק, ידוע וברור כי מערכת המוצעת של הזוכה תשמש רק את משטרת ישראל באתר שיבחר.

7. אבטחת שרתים והקשחות

7.1. שרתי המערכת של הזוכה יאובטחו ויוקשחו באופן שוטף, בפרק זמן סביר מפרסום הטלאים ולפי כללי ה- Best Practice המקובלים בענף.

7.2. הזוכה יתקין אמצעי אבטחה מתאימים בכל השרתים, אשר יכללו לכל הפחות תוכנת אנטי-וירוס ומניעת תוכנה זדונית ומערכת לבקרת סטטוס אבטחת המידע והתראה בפני שינויי קונפיגורציה.

7.3. עמדות הקצה יאובטחו בפני תוכנה זדונית, ובפני הכנסה והוצאת מדיה נתיקה.

7.4. הזוכה יתאים את אמצעי אבטחת המידע לאיומים, כפי שיוגדרו ע"י הזוכה במשותף עם משטרת ישראל מעת לעת.

7.5. הזוכה יתעד כל פעילות בשרתי המערכת באמצעות יומן פעולות (Audit Log) ויבקר אותו כמוגדר בסעיף המתאים במסמך זה.

7.6. הזוכה יאחסן את מדיית הגיבוי באופן מאובטח.

8. אבטחת אפליקציות

8.1. האפליקציות הפועלות במערכת יאובטחו לפי Best Practices מוכרים בשוק, כגון לפי כללי OWASP.

8.2. כל האפליקציות יוקשחו למניעת החדרת קוד זדוני ו/או ניצול פרצות אבטחתיות עקב כתיבת קוד בצורה לא נכונה. לרבות עבור שרתי המערכת, תוכנות במחשבי הקצה וכד'

8.3. אבטחת האפליקציות תתבצע באמצעות יישום אבטחה בקוד.

8.4. פתרונות האבטחה יותאמו לטכנולוגיית היישום, בין אם כמערכת בתצורת שרת לקוח (EXE) או בתצורת דפדפן (Browser).

8.5. הזוכה יתאים את אמצעי אבטחת המידע לאיומים, כפי שיוגדרו ע"י הזוכה במשותף עם משטרת ישראל מעת לעת.

8.6. הזוכה יתאר את מנגנון מידור המידע הלוגי הקיים במערכת, המבטיח מידור מידע מלא בין הגורמים שונים המעורבים בתהליך הלוגיסטי במערכות הזוכה.

8.7. הזוכה ירשום כל פעילות אפליקטיבית חריגה במערכת באמצעות יומן פעולות (Audit Log) ויבקר אותו כמוגדר בסעיף המתאים במסמך זה.

9. אימות זיהוי משתמשים מול מערכות הזוכה

9.1. כל עובד של הזוכה ישתמש בחשבון משתמש וסיסמא אישיים בלבד בגישה לכל מערכת או בסיס נתונים, ולא ייעשה שימוש כלשהו בחשבונות משתמש משותפים, לרבות עבור חשבונות ניהול פריבילגיים.

9.2. מנגנון אימות זהות המשתמשים יהיה מבוסס שם משתמש וסיסמא.

9.3. על הספק לפרט את המנגנון לזיהוי ואימות משתמשים. במידה והמערכת אינה תומכת באחד או יותר מסעיפי הדרישות, יש לציין זאת במפורש.

9.4. מנגנון זיהוי ואימות משתמש על פי הסטנדרטים והנהלים המוכתבים ע"י המשטרה.

9.5. במידה וממשק המשתמש מבוסס WEB יש לעבוד ב- SSL.

9.6. המציע יוודא כי ניהול הסיסמאות עונה על דרישות תקן ישראלי 1495 פרק 3 לניהול סיסמאות ברמה הגבוהה, לגבי חוזק סיסמא, תדירות ההחלפה ומניעת חזרה על סיסמאות קודמות.

9.7. המציע יתאר את מנגנון אימות הזיהוי הממומש אצלו, והאם ממומש באמצעות מנגנון בפיתוח עצמי או מנגנון המבוסס על רכיבי מערכת ההפעלה.

9.8. באם ממומש מנגנון אימות זיהוי מבוסס פיתוח עצמי, בו מאוחסנים חשבונות המשתמש בבסיס נתונים טבלאי כלשהו, יפרט המציע כיצד מאובטחים חשבונות המשתמש והסיסמאות בבסיס הנתונים, ויתאר בהרחבה את מימוש מסך ההזדהות, כיצד מוצפנת הסיסמא למניעת דליפתה, בין אם בציתות לתקשורת או בנגישות לבסיס הנתונים בו היא מאוחסנת.

9.9. באם ממומש מנגנון אימות זיהוי מבוסס מערכת הפעלה, יפרט המציע את המנגנון שמימש. במידה וחלקים שונים ממנגנון אימות הזיהוי הינם מפיתוח עצמי כמו לדוגמא אי מימוש מנגנון מבוסס Gina למול AD, יפרט המציע בהרחבה כיצד הגן על כל שלבי קלט הסיסמא ומניעת דליפתה.

9.10. מנגנוני הרשאות- ניהול הרשאות ומתן הרשאות לפי פרופיל משתמשים. המערכת נדרשת לתמוך בניהול הרשאות משתמשים באמצעות מנגנון המכיל קטגוריות לדוגמא: משתמש, קבוצת משתמים, תפקידים במערכת , סוגי הרשאות לקבוצה/ תפקיד: כגון: קריאה, כתיבה, צפייה, עדכון, ביצוע פעולות מסוימות וכדומה.

9.11. על הזוכה לפרט את יכולת ניהול הרשאות : ברמת המשתמש , ברמת קבוצת משתשים, ברמת סוג המידע , ברמת אובייקט (מסך , כפתור , רשומה , שדה) , ברמת קבוצות אובייקטים וכדומה.

9.12. הספק יפרט קיום אפשרות קביעת פרופיל משתמש לכל קבוצה או תפקיד ארגוני ומתן אפשרות לניהול נוח של מערך פרופיל משתמש. פרופיל המשתמש לא יהיו חשבונות משתמש לגיטימיים במערכת אלא ישמשו להקניית הרשאות בלבד.

9.13. יש לפרט אמצעי חלחול ההרשאות שבמערכת (האם שיוך משתמש לקבוצת משתמשים יעביר אליו גם את ההרשאות של הקבוצה, שינוי פרופיל הרשאות ישנה הרשאות לכל מי שמשויך לפרופיל זה וכו').

9.14. על הזוכה לפרט את מנגנוני האבטחה שבהם יתמכו היישומים המוצעים, לפי הנושאים המפורטים בהמשך.

9.15. על המערכת המסופקת לשמור לפחות על עקרונות אבטחת המידע הכלליים הבאים:

9.15.1. קיום מנגנונים מפותחים של זיהוי, אימות והרשאות.

9.15.2. מערכת ההרשאות תפעל על פי העיקרון: "הכול אסור אלא אם כן הוגדר אחרת".

9.15.3. המערכת תקל ככל האפשר על תחזוקתה, ניהול ההרשאות, המשתמשים שלה וכו'.

9.15.4. המערכת תהיה גמישה ככל הניתן, תאפשר שינוי ברירות מחדל, ופרמטרים ע"י מנהל מערכת.

9.15.5. המערכת תהיה נוחה להתממשקות למערכות חיצוניות לצורך יצוא ויבוא נתונים.

9.15.6. המערכת תספק שירותי ניטור, דיווח ופיקוח נאותים.

10. ניהול משתמשים

10.1. הספק יפרט את מנגנוני ניהול המשתמשים של המוצר.

10.2. יצירת מבנה ארגוני חכם במערכת ההרשאות, והיכולת לממשקן לתוכן הרלוונטי בתוך האפליקציה (מאפשר תחזוקה אוטומטית של משתמשים, עפ"י מקומם הארגוני).

10.3. יש לאפשר ניהול קבוצות חכם (קבוצה בתוך קבוצה, קבוצות חופפות וכו').

10.4. יש לאפשר יצירת משתמש ע"י העתקת משתמש, או ע"י העתקת פרופיל משתמש.

10.5. אין לאפשר למחוק משתמשים מהמערכת , במידת הצורך יש לסמן משתמש כלא פעיל

10.6. יש לאפשר הגבלת פעילות עובדים וקבלת משימות לאזורי עבודה ומחסנים.

11. מניעת זליגת מידע

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

11.1.1. מוצר DLP.

11.1.2. הקשחת מערכת ההפעלה בעמדות קצה.

11.1.3. מניעת גישה למדיה ו-USB בעמדות קצה.

11.2. המציע יתחייב להצפין או למדר גישה לכל מידע הנדרש לכך לפי חוק או רגולציה רלבנטית, או לאבטח את המידע באמצעים חלופיים מספקים למניעת זליגתו של המידע, כגון:

11.2.1. הגדרת גישה למידע לפי הצורך לדעת – Need To Know.

11.2.2. הצפנת מספרי כרטיסי אשראי.

11.2.3. הסתרת ספרות כרטיסי אשראי כנדרש (תצוגת 4 ספרות אחרונות בלבד) .

11.2.4. הצפנה ומידור מידע רפואי במידה וקיים.

11.3. המציע יתאר באופן מדויק ככל האפשר כיצד המנגנונים שתיאר לעיל למניעת זליגת מידע מסייעים למידור המידע לפי מודל "הצורך לדעת", כיצד נאכף המידור, וכיצד ניתן לזהות גישה למידע שלא לפי ההרשאות שניתנו לכל עובד.

12. בקרות וביקורות אבטחת מידע

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

12.2. 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.

12.3. 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'.

12.4. כל ממצאי הבקרות, ביקורות, סקרי הסיכונים, מבדקי חדירה וכד' יועבור **למדור אבטחת מידע של משטרת ישראל**.

12.5. 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.

12.6. המציע יתאר בהצעתו את היקף הבקרות המוצע, תדירותם, ואת הגורם המוצע לבצע את הבקרות הנדרשות, ואשר יעמוד בדרישות המפורטות בסעיף זה (11).

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

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

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

12.9.1. תיקון ליקויים קריטיים – יחל באופן מידי ויושלם תוך 4 שבועות לכל היותר.

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

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

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

12.10. המציע יצרף להצעתו אישור של חברת ייעוץ מוכרת או גורם אבטחת מידע מוסמך (CISSP/CISM) אשר ביצע **במהלך השנה החולפת סקר אבטחת מידע על המערכת הקיימת של המציע**, ומצא אותה עונה על הדרישות המובעות במכרז זה.

12.11. המציע יציג תוכנית תגובה לאירועי אבטחת מידע שמזוהים, כולל כל ניסיון חדירה או דליפה של המידע המוחזק של משטרת ישראל, וכל ניסיון חדירה או דליפה אחר למערכות הספק, שאיננו קשור ישירות למידע של משטרת ישראל.

13. הבטחת רציפות השירות והיערכות לשעת חירום

13.1. המציע יפרט מהם האמצעים והפתרונות המוצעים על ידו להבטחת רציפות השירות במערכות המחשוב שלו. יש לפרט מהם האמצעים הקיימים כיום, ואילו אמצעים ייושמו לטובת הצעה זו לדוגמה:

13.1.1. גיבויים

13.1.2. יתירות שרתים ורכיבי תקשורת – Redundancy

13.1.3. Load Balancing

13.1.4. כפילות קווי תקשורת

13.1.5. אמצעים נוספים

14. ציוד מחשוב של משטרת ישראל במתקן הזוכה

14.1. המציע יאפשר התקנת ציוד מחשוב לרבות מחשבים, ציוד תקשורת, תשתית פסיבית וכל ציוד אחר הנדרש לעבודה השוטפת של יחידת הפיקוח במתקן הזוכה.

14.2. המציע מתחייב לעמוד בכל דרישות והנחיות האבטחה הפיזית הקשורות להתקנת התשתיות הנ"ל שיועברו על ידי הגורם המקצועי המוסמך במשטרת ישראל.

נספח 5 ד' - מפרט תהליכי עבודה במערכת ERP/SAP ומערכת פלא / מג'יק למול מערכת מידע של הזוכה

תוכן העניינים

1. כללי 45
2. מילון מונחים 46
3. שיטת העבודה הכללית 47
4. בקרת ממשקים 48
5. רמת שירות טכנולוגי-SLA 48
6. הקמת תשתיות המערכת 49
7. העברה ראשונית של נתונים למרלו"ג 50
8. דוחות בקרה לנתוני המעבר 51
9. תהליכי עבודה במערכת 51
10. דוחות 55
11. היסטוריית פעילות שינויים 57
12. תנועות שגויות 57
13. סודיות המידע 57
14. מבחני קבלה 58
15. גורמים מעורבים 58
16. תיחום מערכת המחשוב 58
17. בעלות על המידע 59
18. גבולות אחריות 59
19. מערכות RFבמתחם 59
20. שרתים ואחסון מידע 59
21. גיבוי שחזור וזמינות המידע 59
22. שרידות וחוסן המערכת 59
23. ניהול סיכונים 59
24. צוות מערכות מידע של הזוכה 59
25. בדיקות קבלה למערכת ולממשקים 60
26. מערכת הדרכות והטמעה כולל תיעוד 60
27. אופן הגישה למידע 60
28. תוכנה-סוגי רישוי ורשימת תוכנות 60
29. שינויים והתאמות בתוכנה 60
30. תוכנית עבודה ליישום הפרויקט ועליה לאוויר 61

1. כללי

1.1 מערכת ERP/SAP

א. משנת 2010 כלל תהליכי הרכש והמלאי במשטרת ישראל מנוהלים במערכת ה-ERP/SAP המשטרתית

מעבר לכך מערכת ה- ERP/SAP מהווה פלטפורמה ארגונית ואינטגרטיבית לניהול
כלל משאבי הארגון.
בהיבט הטכנולוגי, כל תהליכי העבודה התשתיות והפיתוחים מבוצעים תחת קורת גג של מערכת אחת.
להקמת מרלו"ג אחוד במשטרת ישראל , יש השפעה דרמטית על תהליכי העבודה התקציביים, הפיננסיים והלוגיסטיים ,על אחת כמה כאשר מדובר בעבודה מול גורם חוץ בעל מערכות ניהול עצמאיות.

ב. על-מנת לתת את הפתרון האופטימלי בתפעול המרלו"ג יש צורך בהגדרת הממשקים והגדרת גבולות גזרה של כל גורם בתהליך העבודה.
מערכות המחשוב של הזוכה שייבחר , צריכות להתבסס על העובדה שמערכת ה-ERP המשטרתית היא המערכת המובילה והקובעת בכל הקשור לניהול רמות המלאי וערכי המלאי וכדומה.

ג. מערכת ה- ERP תנהל את בקשות הרכש והמלאי ותוציא הנחיות בהתאם בנוגע לקליטה וניפוק במלאי והזוכה ישקף נתונים אלו במערכת המחשוב של המרלו"ג

ד. בנוסף להפעלת מסרים בין המערכות , נדרש לפתח מנגנונים לניהול ושמירת רמת עדכניות של בסיסי הנתונים של המערכת המשטרתית ומערכת המרלו"ג באופן כזה שיתנהלו כמערכות צל אחת לשנייה. לציין , שמשטרת ישראל תקבע את מבנה הממשקים, פורמט הממשקים ותדירות הממשקים הנדרשים, כולל מנגנון בקרה וטיפול בשגויים, על מנת לשמור על רמת עדכניות שנדרשת במערכת ה-ERP.

ה. מטרת מסמך זה להגדיר את תהליכי העבודה הקיימים כיום בכל הקשור לניהול ותפעול המלאי במשטרת ישראל על מנת לייצר ממשקי עדכון בין שתי המערכות. כמו כן, המסמך מגדיר את תחומי האחריות וגבולות הגזרה בין המשטרה ובין הזוכה.

ו. כפועל יוצא מניהול ממשקים בין שתי מערכות המחשוב, נדרש להקים/לנהל מנגנון בקרה ומעקב של תעבורת הנתונים מ/אל הכספות וכן להפיק דוחות בקרה בהתאם.

ז. כחלק משלבי ההתארגנות והקמת התשתית, נדרש לבצע העברה של מלאי, ממחסני ותחנות משטרת ישראל אל מחסן המרלו"ג. המידע המחשובי על העברת המלאי יוגדר ויפורט בהמשך ויתבצע במסגרת הממשקים שיוגדרו ויפורטו בהמשך.

ח. בנוסף לממשקים בנוגע לתהליכי המלאי, נדרש לנהל מידע בכל הקשור לשינוע ואספקת המלאי בשתי מערכות המחשוב, הן המשטרתית והן מערכת המרלו"ג.

ט. ניהול טבלאות הבסיס והתשתית הינם באחריות המשטרה ויועברו מעת לעת, כפי שיקבע בהמשך, מול זוכה המרלו"ג.

י. מסמך זה דן **<u>בעקרונות</u>** נושאי המחשוב בלבד ואינו מפרט פירוט יתר לנדרש מבחינת מערכות מידע . השלב המפורט יתבצע בשלב הבא של ניהול המכרז.

1.2 <u>מערכת פלא</u>

א. מערכת הפל״א של משטרת ישראל מנהלת את כלל תיקי החקירה והמוצגים בתיק.

ב. בהיבט הטכנולוגי, כל תהליכי העבודה התשתיות והפיתוחים מבוצעים תחת קורת גג של מערכת אחת. מערכת המג״ק במשטרה מנהלת את מעבדות המז״פ .

ג. על-מנת לתת את הפתרון האופטימלי בתפעול המרלו״ג יש צורך בהגדרת הממשקים והגדרת גבולות גזרה של כל גורם בתהליך העבודה.
מערכות המחשוב של הזוכה שייבחר , צריכות להתבסס על העובדה שמערכת הפל״א המשטרתית היא המערכת המובילה והקובעת בכל הקשור לניהול המוצג , השמדות וכד׳.

ד. מערכת פלא תנהל את בקשות האחסון במרלו״ג וכן את ההחלטה לגבי החזרת המוצג / השמדתו וכד׳. הזוכה ישקף נתונים אלו במערכת המחשוב של המרלו״ג.

2. <u>מילון מונחים לנספח זה</u>

מושג	משמעות
אתר לוגיסטי	קוד במערכת ה- ERP המאפשר סימון של יחידות כמו מחוז ו/או מחסני הפצה אזוריים
אתר אחסון	קוד במערכת ה- ERP המסמל מחסן לוגי
העברה בשני שלבים	תהליך עבודה להעברת מלאי שמבטא תנועת שליחה(שלב 1) ותנועת קבלה(שלב 2)
ספק	רשומת אב של גורמים שמבטאת עובד במשטרה או ספק שירותים/טובין
יחידה ארגונית	יחידה/גוף במשטרה שמורשה לבצע פעולות מלאי כניסה/הוצאה/העברה
סוג הזמנת רכש	קוד מערכת SAP המסמן את אופי פעילות הרכש הנדרשת לאותו סוג הזמנה
סוג תנועה	קוד מערכת SAP המבטא פעילות למלאי לדוגמא – הכנסה למלאי /סטורנו להכנסה (102/101)
סוג מסמך מלאי	מסך מלאי המכיל כותרת שורות במערכת SAP המבטא פעילות למלאי-כניסה/הוצאה/העברה
הנחיות	סוג מסמך המאפשר העברות מלאי בין גורמים
כספת	תוכנה המאפשרת הכנסה והוצאה של קבצי נתונים מ/אל המשטרה.
ערכות ניפוק	ערכה ייעודית קבועה לאוכלוסיות ייחודיות במ״י.
מערכת הפל״א	מערכת המנהלת את כלל תיקי החקירה במשטרת ישראל כולל מידע וניהול מוצגים
מערכת המג״ק	מערכת המנהלת את עבודת המז״פ במשטרה כולל בדיקת מוצגים
מוצגים	פריטי תחום המוצגים המשפטיים.

רשם	נציג המשטרה העוסק בעולם הרישום הפלילי ו/ או ניהול מחסן מוצגים (ביחידות בהם קיים מחסן מוצגים ובמרלו״ג).
מוצג	נקרא גם בשם ״תפוס״. כל חפץ לרבות כסף, תעודה, מסמך או בעל חיים שנתפשו ע״י המשטרה או הגיעו לידה, ונקבע כי הם מהווים מוצג בתיק החקירה.

<u>שיטת העבודה הכללית</u>

א. התקשורת בין משטרת ישראל לבין זוכה המרלו״ג תיעשה באמצעות העברת נתונים בכספת.

ב. הקבצים בין הגופים יועברו באמצעות מנגנון הכספות כפי שמוגדר ומפורט בנספח אבטחת מידע המצורף למכרז.

ג. תפעול המרלו״ג יתנהל במערכת מחשוב הזוכה ומערכת המרלו״ג תעדכן את ה- ERP בתנועות המלאי בסיום ביצוע של כל הפעולה וכמו כן , מערכת המרלו״ג תעדכן את מערכת הפלא בסיום ביצוע של כל הפעולה.

ד. כשלב מקדים לתהליכי העבודה השוטפים, יבוצע שלב העברת המלאי וכן מוצגים. תנועות המלאי ותנועות המוצגים בשלב המעבר יבוצעו אף הם בממשקים שיקבעו ע״י המשטרה.

ה. לטובת בניית תהליכי עבודה בין המשטרה ובין זוכה המרלו״ג , יש צורך בהעברת קבצים/נתונים אשר יכילו את המידע בנושאים השונים:

ה.1. נתוני תשתית (נתוני אב).

ה.2. כניסות מלאי למרלו״ג.

ה.3. יציאות מלאי ממרלו״ג.

ה.4. עדכוני מלאי במרלו״ג

ה.5. קבלת מוצגים למרלו״ג.

ה.6. יציאות מוצגים ממרלו״ג.

ה.7. מוצגים שמיועדים להשמדה

ה.8. קבצים שונים כפי שיוחלט בתיאום בין משטרת ישראל לבין זוכה המרלו״ג.

ו. כל פעילות של העברת קבצים/נתונים בין שתי מערכות המחשוב , תלווה בבקרה על התהליך.

ז. בכוונת המשטרה לבצע את העברות המלאי בשני שלבים, כפי שיפורט בהמשך. יש להיערך לאופן העברת המסרים והסינכרון ביניהם.

ח. נדרש להיערך לכך שחלק מתהליכי העבודה יחייבו אישור גורם משטרתי בטרם יבוצע עדכון בין מערכות המחשוב, כלומר, תהליכי עבודה אלו יחייבו מנגנון אישורים כ- WORKFLOW בשתי מערכות המחשוב.

ט. מכיוון שהמערכת הקובעת לכל נושא ניהול המלאי ורמות המלאי , הינה מערכת המחשוב המשטרתית, המרלו״ג יוגדר בתוך ה- ERP כאתר נוסף במערכת ואליו ישוייכו מספר אתרי אחסון (כפי הנדרש) שמהווים סימול וייצוג של מחסן ביניים בתוך האתר.

י. שינוי במבנה הקבצים לניהול תהליכי המשטרה והממשקים ייעשה אך ורק לאחר תיאום עם משטרת ישראל ובהסכמתה.

יא. שינוי במבנה טבלאות תשתית או בתכולתם ייעשה רק בתיאום עם משטרת ישראל ובהסכמתה.

יב. זוכה המרלו״ג מתחייב לאבטח את נתוני המידע, לשמור עליהם ולא לפרסמם, כמפורט בסעיף <u>״סודיות המידע״ וכן בנספח אבטחת מידע המצורף למכרז.</u> אבטחת המידע כוללת גם את תעבורת הנתונים בין משטרת ישראל לבין זוכה המרלו״ג, כפי שמפורט בסעיף <u>״ממשקים והעברת נתונים״.</u>

בקרת ממשקים

א. כל תעבורת הנתונים בין מערכת ה- ERP ובין המרלו״ג תתבצע באמצעות מסרים וממשקים. הן בשלב ההקמה והן בשלב של העבודה השגרתית.
ב. המסרים מ/אל המרלו״ג יעברו דרך תווך של כספות.
ג. נדרש להקים מנגנון/מערכת שתבקר את כל תעבורת הנתונים כולל ניהול הסטאטוס של המסר (הצלחה/כשלון) שנשלחים/מתקבלים בין שתי המערכות.
ד. המערכת תהיה ידידותית למשתמש הקצה שינהל ויפקח על תעבורת המסרים, תקינות השרתים הכספות ושאר רכיבי התשתית שבתווך. המערכת תשמש כקוקפיט בקרתי.
ה. מערכת בקרת ממשקים תנהל היסטוריה של מסרים עם הסטאטוס הרלוונטי.
ו. המערכת תאפשר הפעלה מחדש למסר שנפל ולא נקלט במערכות המחשוב.

רמת שירות טכנולוגי-SLA

2.1 כללי

א. מערכות הזוכה והממשקים צריכות להיות זמינות אל מול מערכות משטרת ישראל. מערכות אלו זמינות ופעילות 24/7 בכל ימות השנה.
ב. בעיתות חירום המרלו״ג יפעל כפי שהוגדר במכרז, הדבר משליך גם על זמינות המערכות והממשקים בהתאמה.

2.2 אירועי תקלות במרלו״ג

במצב שגרה

א. בקרות תקלה בזמן שגרה במערכות זוכה המרלו״ג ו/או בממשקים את מול מערכות משטרת ישראל, אזי, תחילת הטיפול בתקלה ע״י הזוכה במהלך ימי העבודה יתחיל בתוך פרק זמן שלא יעלה על
   א.1. חצי שעה – כאשר אירוע התקלה התחולל בין השעות 7:00-18:00
   א.2. שעתיים - כאשר אירוע התקלה התחולל החל מהשעה 18:00

במצב חירום

א. עם הכרזת מצב חירום על ידי משטרת ישראל, כל תקלה במערכות הזוכה ו/או בממשקים אל מול מערכות משטרת ישראל, תטופל על ידי צוות הזוכה במיידי, כאשר תחילת הטיפול בתקלה יתחיל תוך פרק זמן שלא יעלה על 20 דקות מרגע אירוע התקלה.

תקלות ושדרוגים במערכות המשטרתיות

א. הטיפול בתקלות במערכות המשטרתיות ושדרוגן, הינו באחריות משטרת ישראל.
ב. יחד עם זאת, במידה ויידרש שיתוף פעולה של הזוכה בבדיקות ו/או תיקונים של הממשקים בין מערכות המחשוב הן של זוכה המרלו״ג והן משטרת ישראל, ידרש הזוכה להעמיד צוות מקצועי לביצוע בדיקות ו/או תיקונים הנדרשים.
ג. במקרה של תקלה, זמינות הצוות המקצועי תהיה בהתאם למפורט לעיל.

ד. במקרה של שידרוג, הבדיקות יתבצעו בשעות העבודה השגרתיות ובתאום מראש.
ה. יתכנו מצבים בהם התקלה עלולה להמשך מעבר לזמנים שהוגדרו לעיל, במקרים אלו זמן ההשבתה של מערכות המידע יהיו בידיעה ובאישור של משטרת ישראל.
ו. סיום טיפול בתקלה יהיה על פי הגדרת המשטרה ולשביעות רצון מצד מערכות מידע של המשטרה.

הקמת תשתיות המערכת

2.3 כללי

א. קבצי התשתית יועברו בין משטרת ישראל ובין הזוכה הזוכה, כחלק מחייב בתחילת הפעלת המערכת אך גם באופן שוטף במסגרת העבודה היומיומית
ב. העברת נתוני תשתית אלו יועברו אל הזוכה באופן שוטף בכל מקרה בו יחול עדכון/שינוי כלשהו בנתוני המערכת המשטרתית.
ג. תדירות הפעלת ממשקי התשתית להעברת הנתונים במסגרת העבודה השוטפת וכן שעות ההפעלה שלהם יסוכמו בין משטרת ישראל לבין זוכה המרלו"ג.
ד. נתוני התשתית של משטרת ישראל יכולים להשתנות מעת לעת , תוספת של נתוני תשתית או ביטול חלקי של נתון תשתית ישפיע גם על הממשקים ותעבורת הנתונים. זוכה המרלו"ג נדרש להיערך לשינויים אלו במסגרת המכרז.
ה. העברת קבצי הנתונים תתבצע באמצעות ערוץ מתווך ("כספת" CYBER ARK) כפי שמפורט בנספח אבטחת מידע המצ"ב. זוכה המרלו"ג יטמיע במערכותיו ועל חשבנו את האפליקציות והתוכנה הנדרשים להעברה ולקריאה אוטומטיים של הנתונים בהתאם למפורט בנספח זה.
ו. באופן כללי, אלא אם נאמר או סוכם במפורש אחרת, כל קבצי הממשקים יהיו מסוג קבצי XML.
ז. במקרים מיוחדים, כאמור, ובהסכמת משטרת ישראל ניתן להגדיר קבצי ממשק מסוג אחר או מכל פורמט אחר שיוסכם על שני הצדדים
ח. להלן יפורטו קבצי הממשקים הידועים כיום. חשוב לציין, שייתכן שבמהלך היישום יתברר שיהיה צורך בבנייה של קבצי ממשק נוספים.
ט. מבנה הקבצים המתואר להלן משקף את הידוע למשטרת ישראל בעת כתיבת מסמך זה. המבנה הסופי יתואם בין משטרת ישראל לבין מפעיל המרלו"ג שיזכה במכרז.

2.4 נתוני תשתית

א. לצורך ניהול התשתיות וכחלק מפעילות הקדם של הפעלת מערכות המחשוב ינוהלו , במערכת זוכה המרלו"ג , טבלאות תשתית של משטרת ישראל כאשר המטרה היא ליצור רפליקציה תשתיתית שתשמש את המערכת בעבודה השוטפת במרלו"ג לטובת משטרת ישראל.
ב. רשימת טבלאות התשתית שינוהלו:
   ב.1. נתוני בסיס של קטלוג הפריטים – (כולל פרופיל קטלוג)
   ב.2. נתוני אב של רשימת הספקים של משטרת ישראל– קוד + תיאור
   ב.3. רשימת אתרים המייצגים מחוזות בהיבט הלוגיסטי
   ב.4. רשימת אתרי אחסון (נדרש להשלים כתובות פיזית לאספקה + איש קשר + טלפון)
   ב.5. הנחיות משיכה פתוחות
   ב.6. הזמנות רכש פתוחות כולל מועדי אספקה

ב.7. וכן טבלאות תשתית נוספים שיוגדרו בהמשך ולפי הצורך יחד עם זוכה המרלו״ג

2.5 שגויים בקליטת נתוני תשתית

א. קבצי התשתית מחייבים קליטה מלאה של הנתונים. כלומר, בעת הקמת נתוני התשתית, לא תתאפשר קליטה חלקית של הנתונים במערכת זוכה המרלו״ג, אלא הכל או לא כלום. במקרה של אי הצלחה, יש לטפל בשגויים בהתאם.

ב. במקרה של שגויים, יועברו למשטרה סיבות השגיאה של אי הקליטה, בממשק או בכל דרך שיוסכם עליה בהמשך, על מנת לבצע תיקון וקליטה חוזרת ומלאה של כלל הנתונים.

2.6 אבטחת מידע לנתוני תשתית

א. בהתאם למפורט בנספח אבטחת מידע המצורף למכרז.

2.7 דוחות בקרה לנתוני תשתית

א. זוכה המרלו״ג יאפשר הפקת דו״חות והעברתם למשטרת ישראל במספר חתכים שונים בהתאם לדרישה על מנת לוודא קליטת נתוני תשתית תקינה. הפקת הדו״חות תהיה חלק אינטגרלי מהדרישות במכרז זה.

ב. הדו״חות יופקו בכל פורמט שידרש/שיאושר על ידי המשטרה ובאופן כזה שבאמצעותו תהיה אפשרות לנציגי המשטרה לבצע ניתוח ועיבוד עצמאיים.

ג. העברת הדוחות אל המשטרה תתבצע בכל פורמט שיקבע ע״י המשטרה.

ההעברה ראשונית של נתונים למרלו״ג

2.8 כללי

א. שלב המעבר הוא שלב בו המשטרה תעביר מלאים ממחסנים שונים הפזורים ברחבי הארץ אל המרלו״ג שיקבע.

ב. נתוני המלאי המועבר יועברו ממשטרת ישראל אל הזוכה, כשלב מחייב לפני תחילת הפעלת המערכת אך גם באופן שוטף במסגרת העבודה היומיומית.

ג. ההעברה הראשונית של המלאי / מוצגים תתבצע רק לאחר סיום הקמת כל מערכות הממשקים הנדרשות לטובת הפעלת המרלו״ג ולאחר בדיקות ואישור של המשטרה לגבי תקינות הנתונים.

ד. העברת נתוני המעבר יועברו אל הזוכה בכל מקרה בו יחול עדכון/שינוי כלשהו בנתוני המערכת המשטרתית ובכל מקרה בו המשטרה מצאה לנכון להעביר נתונים אלו.

ה. תדירות הפעלת ממשקי המעבר יתבצעו במסגרת שעות העבודה השוטפת וכן בשעות ההפעלה שבהם יסוכמו בין משטרת ישראל לבין זוכה המרלו״ג וכן בתדירות שתקבע ע״י המשטרה וזאת בגין מקרה של תקלה או בגין אירוע כלשהו כנדרש ע״י המשטרה.

ו. העברת נתוני המעבר תתבצע בפורמט שיקבע ע״י המשטרה.

ז. באופן כללי, אלא אם נאמר או סוכם במפורש אחרת, כל קבצי הממשקים יהיו מסוג קבצי XML.

ח. במקרים מיוחדים, כאמור, ובהסכמת משטרת ישראל ניתן להגדיר קבצי ממשק מסוג אחר או מכל פורמט אחר שיוסכם על שני הצדדים.

2.9 נתוני המעבר

א. תקבע רשימה של אתרי אחסון למעבר ע"י גורמי משטרה.
ב. תתבצע העברת מלאי במערכת ה- ERP המשטרתית.
ג. יועבר קובץ/דוח שבו יצויין המלאי שהועבר לאתר מרלו"ג (במערכת ה- ERP).
ד. תתבצע קליטת הקובץ במערכת המלאי של המרלו"ג.
ה. יופק דוח השוואתי בין הנתונים ב- ERP ונתוני המוצגים ובין הנתונים שהועברו למרלו"ג.
ו. במידה ויש שגויים, נדרש לטפל בהם, כאשר האחריות לשגויים תחול על זוכה המרלו"ג אלא אם יוסכם אחרת ע"י נציגי המשטרה.

2.10 שגויים בקליטת נתוני המעבר

א. במקרה של שגויים בנתוני המעבר, יועברו למשטרה סיבות השגיאה, על מנת לבצע תיקון וקליטה מלאה של כלל הנתונים.
ב. הטיפול בשגויים יסתיים רק כאשר המשטרה תקבע שאכן הטיפול בוצע לשביעת רצון המשטרה.

2.11 אבטחת מידע לנתוני המעבר

א. בהתאם למפורט בנספח אבטחת מידע המצורף למכרז.

דוחות בקרה לנתוני המעבר

א. זוכה המרלו"ג יאפשר הפקת דו"חות עבור משטרת ישראל במספר חתכים שונים בהתאם לדרישה על מנת לוודא קליטת נתוני תשתית תקינה. הפקת הדו"חות תהיה חלק אינטגרלי מדרישות הזוכה במכרז זה.
ב. הדו"חות יסופקו בפורמט אקסל או כל פורמט אחר שיאושר על ידי המשטרה ובאמצעותו תהיה אפשרות לנציגי המשטרה לבצע ניתוח ועיבוד עצמאיים.

תהליכי עבודה במערכת

2.12 כללי

א. פרק זה מפרט את התהליכים המרכזיים בניהול המלאי של מערכת ה- ERP ומערכת הפלא / מג"ק אל מול זוכה המרלו"ג.
ב. כפי שצויין, המרלו"ג יוגדר במערכת ה-ERP המשטרתית כעוד אתר שבו מנוהל המלאי המשטרתי. על כן כל פעילויות המלאי במרלו"ג מחייבות ביטוי גם במערכת ה-ERP.
ג. עבור כל תהליך שיפורט בהמשך, יש לתת בעבורו ביטוי באמצעות ממשקים באופן זהה לממשקים שצוינו בנושא קבצי התשתית.

ד. על מנת ליצור סינכרון והתאמת מלאי בין מערכת המרלו"ג ומערכת ה- ERP תתבצע בכל לילה ריצת התאמת מלאי באמצעות הפקת קבצים משתי המערכות במטרה לבצע הצפת פערים וטיפולם.

ה. מסמך זה מציין את התהליכים המרכזיים, אך יתכן שיתווספו תהליכי עבודה נוספים שיידרש לתת להם מענה במסגרת ממשקים נוספים בין מערכות מחשוב של משטרת ישראל ובין מערכת מחשוב של זוכה המרלו"ג, כלומר מסמך זה מציין את רשימת הממשקים העקרוניים אשר תורחב ותאושר בשלב האפיון המפורט.

2.13 פירוט תהליכי העבודה

קבלת טובין במרלו"ג כנגד הזמנת רכש

א. במערכות המשטרה, קבלת טובין חייבת להתבצע כנגד הזמנת רכש.

ב. הזמנת רכש נוצרת במערכת ה-ERP ותועבר אל המרלו"ג, במסגרת הקמה ראשונית של התשתיות וגם באופן שוטף במסגרת העבודה היומיומית הרגילה.

ג. הזמנת רכש יכולה לעבור מספר שינויים (כמות, מחיר וכו'), על כן, נדרש להיערך לכך במערכות המחשוב של המרלו"ג בשמירת היסטורית שינויים בהזמנת הרכש וכן בשמירת הגרסה האחרונה של הזמנת הרכש.

ד. כמו כן, יתכנו שינויים בכמות המסופקת ע"י ספק הטובין, נדרש להיערך לקליטת טובין באופן שלא תחרוג מהכמות המצוינת בהזמנת הרכש, להדגיש לא ניתן לבצע קליטת מלאי מעבר למצוין בהזמנת הרכש.

ה. מערכת המרלו"ג תקבל ממערכת ERP צפי קבלה של מועד האספקה כפי שמצוין בהזמנת הרכש עבור כל משלוח הצפוי להתקבל ולהיקלט במחסן. מועד האספקה יכלול בין השאר את הנתונים הבאים: מק"ט, כמות, ספק, הזמנת רכש, מועדי אספקה ועוד.

ו. מערכת המרלו"ג תאפשר קליטת הזמנות אך ורק בשידור ממערכת ה-SAP. לא יוקלדו הזמנות ישירות ולא יהיה ניתן לבצע עדכון להזמנה כלשהיא במערכת המרלו"ג. כל עדכון הוספה או גריעה של הזמנה יבוצע דרך מערכת ה-SAP ומשם ישודר למערכת המחשוב של זוכה המרלו"ג בתהליך עבודה שוטף.

ז. נדרשת בקרת מסרים על שליחה וקבלת נתוני ההזמנה, כפי שצוין לעיל בנושא בקרת ממשקים של נתוני תשתית.

בקשה לניפוק טובין ממרלו"ג ליחידה

א. התהליך מתבצע באמצעות הנחיות (STO).

ב. תהליך העברת מלאי ממרלו"ג ליחידה יתבצע בשני שלבים. כלומר:

ב.1. המרלו"ג יבצע רישום הוצאת מלאי ממחסן.

ב.2. המלאי יועבר להכנה לשינוע.

ב.3. המלאי בשינוע.

ב.4. היחידה שקבלה את המלאי תבצע את השלב השני, של קליטת המלאי.

כל שלב שצויין לעיל, יועבר אל מערכת ה- ERP.

ג. הנחיות לניפוק מלאי ליחידה שיוצאות ממערכת ה-ERP יכולות להיות עם כמות גדולה מהמלאי הקיים פיזית במרלו"ג. המרלו"ג ינפק רק את הכמות הקיימת פיזית ולא יותר מכך.

ד. נדרש לנהל בקרה על העברות אלו בשתי מערכות המחשוב, כולל ניהול שגויים כפי שמצוין במסמך זה.

<u>החזרת טובין מיחידה למרלו"ג</u>

א. התהליך מתבצע באמצעות הנחיות (STO).
ב. תהליך העברת מלאי מיחידה למרלו"ג יתבצע בשני שלבים. כלומר:
ב.1. היחידה תבצע רישום הוצאת מלאי ממחסן היחידה.
ב.2. המרלו"ג יבצע את השלב השני של קליטת המלאי.
ב.3. כל מלאי שיגיע למרלו"ג יכנס לאתר אחסון בלאי בלבד. מלאי זה יעבור בחינה של נציגי משטרת ישראל והם בלבד יחליטו לגבי המשך הטיפול בו.

כל שלב שצויין לעיל, יועבר אל מערכת ה- ERP. כולל שלב שינוע הפריטים.
ג. נדרש לנהל בקרה על העברות אלו בשתי מערכות המחשוב, כולל ניהול שגויים כפי שמצוין במסמך זה.

<u>השמדה/גריטה של ציוד</u>

א. תהליך זה יתבצע במערכת ה- ERP אולם כל תנועה של הציוד במרלו"ג תעבור אל ה- ERP.
ב. הכנת המלאי להשמדה/גריטה תתבצע בחצרות המרלו"ג ובמערכת ה-ERP המשטרתית בכפוף לוועדת הבלאי.

<u>ליקוט פריטים ושינוע ללקוח</u>

א. תהליך הליקוט שיתבצע במרלו"ג מחייב הנפקת שובר ממערכת ה-ERP.
ב. תהליך הליקוט ינוהל עפ"י סטאטוסים. לדוגמא –
ב.1. תחילת ליקוט
ב.2. איסוף
ב.3. סגירת ליקוט
ג. סטאטוסים אלו יעברו אל מערכת ה- ERP בפורמט שיקבע בהמשך.

<u>ספירות מלאי במרלו"ג ע"י הזוכה</u>

א. שיטת ספירת המלאי באזורי האחסון השונים של המחסן תקבע בשלב האפיון המפורט.
ב. אופן ביצוע הספירות יעשה על ידי מסופון או באמצעות מסכי המערכת או כל אמצעי שיקבע ובתנאי שהגורם הוא מורשה לכך.
ג. כחלק מנתוני התשתית של הקטלוג, יוגדר בקטלוג מחזוריות ספירות לפריט. נתון זה יועבר למרלו"ג במסגרת ממשקי נתוני התשתית השוטפים.
ד. יש לצורך ליצור רפליקציה של תהליך הספירה, שתתבצע במרלו"ג, במערכת ה- ERP. לצורך כך יעברו כל מסמכי הספירה עם הפרטים הרלוונטיים אל המערכת המשטרתית החל מפתיחת הספירה, שלבי הספירה, טיפול בהפרשים, וסגירת הספירה.
ה. הספירה תהיה ברמת המק"ט/פריט ולא ברמת האיתור במרלו"ג.

ו. גם כאשר נספרו פריטים במרלו״ג ולא נמצא הפרש כלשהו, על נתון זה להגיע אל מערכת ה-ERP.

ז. ספירה חוזרת – במקרה של חוסר התאמה בין הכמות המדווחת לכמות הרשומה ב-WMS, יידרש טיפול נפרד על פי נוהלי המשטרה.

ח. על המערכת לתעד ולהעביר נתוני תשתית ספירה, כמו אוכלוסייה שנספרה, סוג הספירה, יוזם הספירה, תאריך, תוצאות הספירה ועוד.

ט. פריט מנוהל אצווה - בעת ביצוע הספירה המשתמש יידרש להזין אצווה / לאשר אצווה מוצגת.

י. ספירות לפריטים המנהלים מספר סידורי – המערכת נדרשת לסרוק מיקום, פריט ולהציג את כל המספרים הסידוריים ברצף ,האישור נעשה על ידי סריקה או הקלדה של הסידורי.

יא. ספירות בעודף למספר סידורי שלא קיים במערכת – מלאי מסוג זה יכנס לסטאטוס או איתור ייעודי לניהול הפרשי המלאי. המשתמש יצטרך להזין תוקף/ אצווה במידה ומנוהל.

יב. מלאי של פריט שנמצא במרלו״ג עם יתרה אך היתרה במערכת ה-ERP לא קיימת, רק משתמש מורשה יבצע התאמות בין המערכות.

יג. על המערכת לאפשר להגדיר זמן ליצירת התראה על מלאי הנמצא בסטאטוס ״הפרשים״ מעל לפרק זמן שיקבע בשלב האפיון המופרט, משום שהדבר משפיע על מערכת ה-ERP באופן חשבונאי.

יד. המערכת נדרשת להפיק דוח של פריטים שלא נספרו בטווח התאריכים לבחירת המשתמש.

טו. המערכת תתמוך בהפקת דוחות על התקדמות הספירות וביצוע הספירות אשר יאופיינו בשלב האפיון המפורט.

טז. המערכת תאפשר לבקר אחר התקדמות משימות הספירה ע״י שאילתות ודוחות ייעודיים כפי שיפורטו באפיון המפורט.

יז. כל הספירות ירשמו בהיסטורית הפעילות של המערכת כולל איתור, תאריך וזמן הספירה, שם הסופר, הכמות שהייתה צפויה, נספרה וההפרש.

<u>איזון ספירות (טיפול בהפרשי ספירה)</u>

א. דיווח איזון ספירה במערכת ה- ERP מחייב אישור גורם משטרתי.

ב. האיזון יתבצע ע״י גורם משטרתי או מיופה כוחו.

ג. תהליך האיזון הסופי יקבע בהסכמה בין המשטרה כלקוח ובין זוכה המרלו״ג תוך מתן מענה לצורכי המשטרה.

<u>ניהול MRP וקווים אדומים</u>

א. תהליך ה-MRP וכן ניהול הקווים האדומים במלאי יתבצע במערכת ה-ERP, אך זוכה המרלו״ג יקלוט את המידע הרלוונטי בממשק.

ב. מבנה הממשק וסוגי המידע יקבעו בהסכמה בין המשטרה כלקוח ובין זוכה המרלו״ג תוך מתן מענה לצורכי המשטרה.

ג. נושא זה יקבל ביטוי בשלב האפיון המפורט, בהנחיה ובהובלה של משטרת ישראל.

ד. על הזוכה להיערך מבחינה מחשובית ומכל בחינה אחרת להפעלת ה-MRP במשטרה ולהשפעתו על המרלו״ג.

<u>הכנת ציוד למכירה</u>

א. כמפורט במכרז.

קבלת וקליטת מוצגים

א. הספק יבצע תהליך קבלה וקליטת מוצגים אשר יגיעו מתחנות הלקוח או מגורמים אחרים מטעם הלקוח, באמצעות קבלן השינוע למוצגים או כל גורם המוסמך ע״י הלקוח.
ב. הספק יקבל צפי קבלת מוצגים בהתממשקות בין מערכת ה״פלא״ עם מערכת ה-WMS של הספק, לפי תעודת המשלוח שתוקם ע״י הרשם בתחנת המקור.
ג. בעת העברת המשלוח מתחנת המקור לקבלן השינוע ישונה הסטטוס במערכת ל-״במעבר אצל קבלן השינוע״.
ד. עם הגעת קבלן השינוע למרלו״ג, תבוצע קליטת המשלוח ע״י המרלו״ג והסטטוס ישונה ל-״נמסר למרלו״ג״.
ה. עם קליטת המוצגים למרלו״ג ישונה הסטטוס ל-״במרלו״ג״.
ו. עד ההגעה הפיזית של המוצגים למרלו״ג, מערכת הפלא תעביר את תעודת המשלוח באמצעות ממשק ל-WMS ובכלל זה את כל המידע על המוצגים שמועברים למרלו״ג.

ליקוט והכנת משלוחים של מוצגים

א. הספק יבצע ליקוט והכנת משלוחים של מוצגים בהתאם לדרישות שיועברו בממשק ע״י הלקוח למערכת ה-WMS. הדרישות יפרטו את הלקוח (מספר תחנה) ואת המוצגים הנדרשים.
ב. הספק יקבל מקבלן השינוע ארגזי שינוע ואזיקונים לטובת אריזת מוצגים המיועדים לשינוע.
ג. ארגזי השינוע בהם יועברו המוצגים ייסגרו באזיקון מסומן (״פלומבה״) בטרם המסירה והשינוע.
ד. המספר הסריאלי של האזיקון המסומן יועבר מתחנת המוצא לתחנת היעד באמצעות ממשק במערכות המידע, ויאומת ע״י מקבל הארגז בהגיעו ליעד.

ליקוט והכנה להשמדת מוצגים

א. הספק יבצע ליקוט של מוצגים אשר הלקוח אישר כי הם נדרשים להשמדה. הלקוח יעביר בממשק למערכת WMS של הספק את רשימת המוצגים כדי שילקט וירכז אותם לפני ביצוע ההשמדה.

קבלת מוצג (מסוג סמים) ישירות ממעבדת הסמים שתוקם במרלו״ג

א. הספק יבצע תהליך קבלה וקליטת מוצגים אשר יגיעו ממעבדת הסמים שתוקם במרלו״ג וכל זאת באמצעות ממשקים למערכת המג׳ק ומערכת הפל״א .

דוחות

א. המערכת תכלול מחולל דוחות, המאפשר גישה ובניית דוחות על פי כל ישויות המערכת והמאפיינים שלהם.
ב. השימוש במחולל יהיה מוגבל למשתמשים מורשים בלבד ולנציגי חוליית הקישור.
ג. הבנייה וההפקה של הדו״חות תהיה פשוטה וידידותית למשתמש.
ד. המערכת תתמוך בהפקת דוחות, מדבקות ומסמכים המכילים נתונים בעברית ותאפשר ייצוא הפלטים לקובצי אקסל.
ה. תתאפשר הפקת דוחות אוטומטיים בקצבי זמן קבועים והתראות שונות ושליחתם למייל או טלפון המשתמשים.

ו. רמות ההצגה של הדו״חות, החיתוכים המדויקים, השדות וכל יתר המרכיבים המהווים חלק בלתי נפרד מאפיון הדו״חות, יאופיינו בשלב האפיון המפורט יחד עם הזוכה שייבחר.

ז. המערכת תאפשר הפקה וגזירה של נתונים מהיסטורית הפעילות של המערכת והסטטיסטיקות שלה. על המערכת לאפשר למשתמש יכולת לייצר דוחות ולעדכן דוחות קיימים, לייצא נתונים מדוח או שאילתה לגיליון אקסל.

ח. הדוחות יפעלו באופן שלא ישפיע על תפקוד וביצועי המערכת.

ט. אפיון דוחות המערכת המפורט יקבע במהלך האפיון המפורט של המערכת יחד עם המשטרה, אשר יכללו **<u>לפחות את הדוחות הבאים</u>**:

ט.1. דוח סיכום פעילות חודשי לטובת התחשבנות התשלום.

ט.2. דוח מלאי של פריטים בסטטוסים שונים.

ט.3. דוח רמות מלאי מתחת למינימום הנדרש.

ט.4. דוח ניתוח תנועות פריטים מבחינת שורות ליקוט וכמויות בתקופות זמן משתנות.

ט.5. דוח מלאי ללא תנועות בתקופת זמן משתנה.

ט.6. דוח הפרשים לספירות מחזוריות.

ט.7. דוח אחוזי ספירות מלאי ביחס לתפוסה במרלו״ג

ט.8. כמות הפריטים שנופקו ע״י עובד לפי זמנים יום שבוע וכו׳ .

ט.9. כמות פריטים במלאי – בפילוחים שונים .

ט.10. רמות מלאי במחסן – בכל נקודת זמן, עם הצפה של הפריטים בעלי כיסוי מלאי נמוך מרמת מלאי .

ט.11. כיסוי מלאי לכל הפריטים בחודשים .

ט.12. כמות פריטים לא פעילים – לפי תקופה – ברבעונים .

ט.13. כמות פריטים בעלי תדירות ניפוק גבוהה ואו נמוכה .

ט.14. כמות פריטים המועברת יומית לשינוע .

ט.15. כמות פריטים עם משוב סופי של הלקוח כי התקבלו/ לא התקבלו .

ט.16. כמות הפריטים שלא נמצאו בספירה .

ט.17. כמות קבלות למחסן .

ט.18. המרות במחסן

ט.19. תוספת פריטים במחסן שלא בדרך הרכש .

ט.20. פריטים שנגרטו .

ט.21. פריטים שנמכרו.

ט.22. פריטים שעברו להשמדה.

ט.23. מצב מלאי חירום וקוים אדומים

ט.24. דוחות מסרים שנכשלו בממשק

ט.25. דוחות לפי סטאטוס מסרים במערכת

ט.26. דוח פריטים שהתקבלו.

ט.27. דוח פריטים שנשלחו .

ט.28. דוח פערים בין פריטים שנשלחו ולא התקבלו וההיפך.

ט.29. דוח שרשרת הפריט בהעברתו ממקום למקום בתוך מרלו״ג.

ט.30. פריטים שעברו להשמדה.

ט.31. ועוד

היסטוריית פעילות שינויים

א. המערכת תשמור רישום של כלל הפעילות והשינויים במערכת. היסטורית השינויים תנוהל כך שכל עוד המלאי קיים ומאוחסן במערכת לא תמחק היסטורית הפעילות שלו. המערכת תשמור על נתוני היסטורית הפעילות זמינים לתחקור והפקת דוחות לתקופת זמן כפי שיקבע באפיון המפורט. מידע שיוחלט להסירו לא ימחק אלא יועבר לארכיון או למקום אחר כפי שיקבע.

ב. המערכת תספק יכולת תחקור של הפעילות ההיסטורית לצורך קבלת מענה ותשובות למקרים של חוסרים במלאי או פעולות לא צפויות, הפקת דוחות פעילות ועוד.

ג. סטטיסטיקה של הפעילות במערכת - המערכת תאסוף נתונים סטטיסטיים על סוגי פעילויות שונים בחתכי זמן, פריטים, אזורי אחסון, כמות תנועות, כמות הזזות פנימיות, יעילות עובדים בהשלמת משימות וכו'

תנועות שגויות

א. תנועה שגויה היא למעשה, כל טרנזקציה/פעולה הקשורה לעניין מכרז זה שלא נקלטה במערכות המחשוב של משטרת ישראל.

ב. תנועה שגויה שלא תיקלט במחשבי המשטרה, תנוהל בקובץ שגויים להמשך טיפול.

ג. חלק מטיפול בתנועה שגויה הוא, הפעלה מחודשת של המסר שנכשל לאחר הטיפול בבעיה.

ד. דוגמאות של תנועות שגויות:

ד.1. בעת העברת מלאי , בשני שלבים, לא נקלט השלב הראשון במערכות מידע.

ד.2. בעת העברת נתוני הנחיה, לא נקלט מועד האספקה באופן תקין

ד.3. ועוד.

סודיות המידע

א. זוכה המרלו"ג מתחייב לשמור על סודיות המידע המגיע אליו במסגרת ביצוע הפרויקט לעניין מכרז זה. ובכלל זה כל המידע הנוגע למשטרת ישראל אופי עיסוקה, אופי עיסוקן של מי מיחידותיה, סידורי הביטחון שלה, מתקניה, ומערכות קיימות אצלה או מערכות בשלבי ההתקנה. ובכלל זה מסמכים בסעיף זה כוללים כל מידע לרבות זה האגור במדיה אלקטרונית.

ב. מודגש בזאת, כי נתוני המלאי, ונתוני התשתיות חומרה ותוכנה מסווגים, ויש לנהוג בהם כאמור במסמכים בסעיף זה.

ג. בעלי זכות החתימה של זוכה המרלו"ג מתחייבים בזה לחתום על מסמך "שמירת סודיות" של משטרת ישראל, ולהחתים עליו את כל מי שמאושר על ידי משטרת ישראל ושיעבוד מטעמם בפרויקט באופן ישיר או בלתי ישיר או מי שתהיה לו גישה לתוכנות, שיטות ונהלי עבודה, מפרטים טכניים, מערכת בטחון וכל חומר רגיש אחר הנוגע לביטחון.

ד. זוכה המרלו"ג מתחייב להחזיק את כל המסמכים לרבות התוכניות והשרטוטים הקשורים לביצוע הפרויקט בארון אחסון אשר נעול ונגיש רק לבעלי תפקיד במשטרה או מי מטעמה הכל על פי הנחיות משטרת ישראל ובהתאם לנוהלי הביטחון של משטרת ישראל, ולעשות את כל הנדרש כדי שהמסמכים הקשורים במ"י ובהתקשרות זו לא יגיעו לגורמים בלתי מוסמכים.

ה. מסמכים שהם רכוש כל אחד מהזוכים או קבלן משנה שלו, אינם מזוהים כקשורים עם התקשרות זו ואין עליהם ציון הקושר אותם ל משטרת ישראל, אינם נכללים בסעיף זה.

ו. האמור בסעיף זה יחול, באחריותו של זוכה המרלו"ג, גם על כל ספקי המשנה איתם יתקשר זוכה המרלו"ג לצורך מימוש אחריותו ותפקידיו לעניין האמור במכרז זה.

מבחני קבלה

א. מבחני הקבלה יכללו:

א.1. בדיקה של שרשרת העברת הנתונים מתחילת אירוע ועד לדיווחו בקבצים השונים.

א.2. בדיקה של נכונות הקבצים המועברים.

א.3. מבחני הקבלה יבוצעו על פי תרחישי פעולות במערכת.

ב. בתקופת ביצוע מבחני הקבלה נדרשת זמינות מלאה של אנשי מערכות מידע של הזוכה ולעבודה בכפיפות לאנשי מערכות מידע של המשטרה וזאת על מנת לממש את מבחני הקבלה לשביעות רצון המשטרה

ג. אישור על סיום מבחני קבלה יינתן לכל התהליכים שיצוינו בהמשך

ד. להלן התהליכים הנדרשים לביצוע מבחני קבלה

ד.1. קליטת נתוני תשתית

ד.2. טיפול בשגויים של נתוני תשתית

ד.3. קליטת נתוני מעבר

ד.4. טיפול בשגוי מעבר

ד.5. בדיקת ממשקי תהליכי עבודה כמפורטים לעיל

ד.6. בדיקת מנגנון בקרת ממשקים

ד.7. טיפול בתורים

ד.8. ניהול שגויים

ד.9. הפקת דוחות שגויים

ד.10. הפקת דוחות תהליכיים

גורמים מעורבים

א. את"ל/ מח"א/ מדור ציוד

ב. את"ל/ מח"א/ חוליית תפעול

ג. יחידות אירגוניות במשטרה

ד. חשבות

ה. ספק השינוע

ו. מנט/מערכת לוגיסטית / מערכת ERP.

ז. מנט/מערכת פלא/מג"ק

ח. מז"פ

ט. חקירות

י. רשמים ביחידות

יא. מעבדות סמים

תיחום מערכת המחשוב

א. ניהול תשתיות.

ב. העברת מסרים/תנועות.

ג. בקרת ממשקים.

בעלות על המידע

א. כל המידע בתחום התוכנה והחומרה הרלוונטי לפעילות המשטרתית במערכת המרלו״ג ובחצרות הזוכה הן במישרין והן בעקיפין, מידע זה הוא רכוש המשטרה ואין לבצע בו שימוש כלשהוא ללא אישור חתום ומפורש תוך ציון אופי המידע, סיווגו ותוקף אישור השימוש בו.

גבולות אחריות

א. המלאי במרלו״ג שייך למשטרה אך מנוהל ע״י הזוכה במרלו״ג.
ב. האחריות לתעבורת הנתונים וקליטתם תחול על זוכה המרלו״ג.
ג. שמירת המידע וההיסטוריה תחול על זוכה המרלו״ג.
ד. זוכה המרלו״ג אחראי לספק כל מידע רלוונטי הקשור לנתוני המלאי של משטרת ישראל.

מערכות RF במתחם

א. מערכות ה-RF שבמתחם המרלו״ג מחייבות בקבלת אישור אבטחת מידע של המשטרה.
ב. דרישות בנושא זה מפורטות בנספח אבטחת מידע המצורף למכרז זה.

שרתים ואחסון מידע

א. כמפורט בנספח דרישות התקשוב של המשטרה.

גיבוי שחזור וזמינות המידע

א. מטרת הגיבויים היא למנוע איבוד מידע כאשר קורה כשל בתקשורת או בעיות מחשוב אחרות.
ב. נדרש לבצע גיבויים עיתיים למידע המשטרתי, באופן כזה שיאפשר שחזור נתונים מהיר יעיל ומדויק ביותר על מנת לא לאבד מידע.
ג. תדירות הגיבויים תיקבע בהמשך מול זוכה המרלו״ג וכפי שמוגדר בנספח דרישות התקשוב.

שרידות וחוסן המערכת

א. כמפורט בנספח דרישות התקשוב.

ניהול סיכונים

א. כמפורט במכרז.

צוות מערכות מידע של הזוכה

א. צוות מערכות המידע יהיה זמין לכל פעילות נדרשת של הצוות המשטרתי.
ב. בכל שלבי פיתוח והתאמות המערכת , הצוות של הזוכה יהיה כפוף ללו״ז הפיתוח של המשטרה.
ג. הזוכה מתחייב להעמיד צוות מתוגבר בתקופת בדיקות הקבלה ובמיוחד בחודשים הראשונים של עליית המערכת לאוויר.
ד. גם בתקופת השגרה, שלאחר עליית המערכת לפעילות שוטפת, צוות הזוכה יחוייב להיות זמין **במיידית** לכל שינוי ו/או תוספות נדרשות למשטרת ישראל.

בדיקות קבלה למערכת ולממשקים

א. במסגרת ההערכות המחשובית, על זוכה המרלו״ג להקים סביבה מחשובית שתהיה ייעודית לבדיקות.
ב. בדיקות תוכנה ו/או ממשקים לא יתבצעו בסביבת היצור, ללא אישור מפורש וכתוב ע״י גורם ממשטרת ישראל.
ג. תבנה תוכנית בדיקות קבלה של הממשקים והפיתוחים בשיתוף עם זוכה המרלו״ג.
ד. בדיקות הקבלה יחולו על כל המרכיבים הנדרשים.
ה. בדיקות הקבלה יתבצעו בשיתוף צוות הבודקים הן של הזוכה והן של המשטרה עבור הממשקים ומערכות הבקרה והדוחות שיפותחו לטובת פרויקט זה.

מערכת הדרכות והטמעה כולל תיעוד

א. הזוכה מתחייב לבצע הדרכות למערכת המידע של המרלו״ג בכל הקשור לניהול ותפעול המערכות בכל עת שהמשטרה תמצא לנכון לבצע הדרכות למי מאנשיה.
ב. הדרכות אלו יתקיימו בסביבה נאותה תוך הקפדה על כל האמצעים הנדרשים לקיים הדרכות והטמעות כמקובל במשטרה לרבות תוכנות עזר ואמצעי תיעוד למערכת.
ג. ההדרכות יתבצעו בסביבה מחשובית הייעודית לכך ולא יתבצעו בסביבת היצור.
ד. כל פעילות בסביבת היצור שאינה לטובת המהלך השוטף של המרלו״ג, יחייב אישור מפורש של משטרת ישראל.

אופן הגישה למידע

א. המידע במערכת המחשוב של המרלו״ג יהיה זמין בכל עת למשטרה.
ב. הגישה תקבע בהמשך אל מול זוכה המרלו״ג.

תוכנה-סוגי רישוי ורשימת תוכנות

א. במידה וזוכה המרלו״ג ביצע שינוי ברישוי ו/או בתוכנת המרלו״ג ו/או כל תוכנה אחרת הנדרשת למשטרה בתפעול המרלו״ג, יש להביא את הדבר לידיעה ולאישור משטרת ישראל תוך ציון ופירוט המשמעויות הנגזרות כתוצאה ממהלך שכזה.
ב. כל שינוי בתוכנה יחייב בדיקות תוכנה ובחינת ההשפעות של המשטרה ועל מערכות המידע המשטרתיות.
ג. בדיקות התוכנה יתבצעו בסביבה ייעודית לכך ורק לאחר אישור מפורש מטעם המשטרה, השינוי יועבר לסביבת היצור לשביעות רצון המשטרה.
ד. בנוסף לכל האמור לעיל, רישוי התוכנות ושימושם יהיה בכפוף להנחיות אבטחת מידע של המשטרה

שינויים והתאמות בתוכנה

א. מפעם לפעם מתבצעים שידרוגים במערכת ה-ERP המחייבים השבתה לפרקי זמן קצרים של מערכת ה-ERP הבאים לידי ביטוי במספר ימים בודדים.
ב. בנוסף לכך, אחת לשנה מתבצע תהליך סגירת שנה המחייב השבתה של מערכת ה-ERP , גם כאן לפרקי זמן קצרים כפי שצויין לעיל.
ג. נדרש מזוכה המרלו״ג להיערך לנושא זה שיכול להתבטא בעצירת ממשקים מצד אחד אך גם שמירת המידע בתור מסרים מצד שני. המסרים ימתינו בתור ויועברו אל מערכת ה-ERP כאשר תחזור לפעול באופן רגיל ושוטף.
ד. זוכה המרלו״ג יערך למנגנון ניהול התורים ולהפקת דוחות לנושא זה, כולל העברת מידע מכל סוג שהוא הקשור להשבתה הנ״ל ולניהול התורים הנ״ל.

<u>תוכנית עבודה ליישום הפרויקט ועליה לאוויר</u>

א. התוכנית תקבע במשותף ובהסכמה עם יחידת המחשוב של זוכה המרלו״ג.
ב. התוכנית תכלול פעילות מקיפה ושלבים מפורטים לעליה לאוויר של כל מערכת הממשקים והעברת הנתונים מ/אל מרלו״ג/ERP תוך ציון לו״ז ומשאבים נדרשים.
ג. תכנית הפעולה תחויב באישור גורמי משטרה.