מסמך אפיון מפורט



**מדינת ישראל**

**משרד הביטחון**

***מסמך איפיון דרישות***

ספק מורשה קשר דיגיטלי

מסחרי

קריטריונים לעמידה בדרישות לספק מורשה לקשר דיגיטלי מסחרי בין משרד הביטחון לביו ספקיו



## תוכן העניינים

[תוכן העניינים 2](#_Toc312833586)

[0. יעדים 3](#_Toc312833587)

[1 תנאים כלליים 14](#_Toc312833588)

[2. יישום – דרישות עיסקיות 18](#_Toc312833589)

[3. טכנולוגיה ותשתית 55](#_Toc312833590)

[4. שירות ו-SLA 59](#_Toc312833591)

[נספחים 66](#_Toc312833593)

## 0. יעדים

### 0.0 כללי

1. המשרד מקיים קשרים עסקיים עם כ-13,000 ספקים ובמסגרת זו שולח ומקבל כ-8 מיליוני מסמכים בשנה (הזמנות, חשבוניות וכו'). המשרד מעוניין לבנות תשתית דיגיטאלית לצורך הרחבת הסחר אלקטרוני מול כל ספקיו.
2. קשרי הסחר האלקטרוני בין המשרד לספקיו יתבצעו באמצעות **מפעילים**. תפקיד המפעיל יהיה לתווך בין הספקים לבין המשרד ולתמוך בשני הצדדים לעמוד ביעדיהם העסקיים באמצעות סחר אלקטרוני.
3. התיווך בין המשרד לספקיו יתבסס על כלים ושירותים שיספק המפעיל, יתפעל ויתחזק לטובת המשרד וספקיו. כלים ושירותים אלה, כמפורט להלן, יאפשרו לצדדים להעביר ביניהם מסרים, ומסמכים אלקטרוניים כדוגמאת הזמנות, חשבוניות, דוחות וצרופות:
4. עסק לעסק (B2B) – פונקציונאליות דומה למוסבר בסעיף א', כאשר הספק עובד במערכות הייעודיות שלו, ומשתמש במימשקים שיפותחו ויתוחזקו ע"י הספק ו/או המפעיל, ואשר יסבו את האירועים למבנה שיוגדר ע"י המפעיל, לצורך העברתם למשהב"ט.
5. פורטל(B2C) – סביבת עבודה באמצעותה יוכלו ספקי המשרד לדווח אירועים עסקיים חדשים כגון חשבוניות, לצפות באירועים עסקיים שמדווחים ע"י המשרד כדוגמאת הזמנות ובמצב הטיפול באירועים עסקיים שאותם יזם המפעיל או המשרד. וכן לעדכן אירועים עיסקיים שגויים.

### 0.1 יעדים ומטרות

#### 1.0.0 יעדים כלליים

1. השגת תשתית לדיגיטציה מלאה של כל תעבורת הסחר האלקטרוני של המשרד.
2. שיפור השירות לספקי המשרד.
3. יצירת סטנדרטיזציה של תהליכי שרשרת האספקה מול ספקי המשרד.

#### 0.1.1 מטרות מעשיות

1. קביעת סטנדרטים אחידים לפעילות המפעילים מול המשרד ולקוחותיו.
2. צמצום היקף העבודה הידנית של עובדי המשרד.
3. הגדלת מספר הספקים הכלולים במערך הדיגיטציה של תהליכי הסחר האלקטרוני.

### 0.2 בעיות

#### 0.2.0 תמצית הבעיות במצב הקיים

1. המשרד משקיע עבודה ידנית רבה בקליטת חשבוניות המוגשות במסמכי נייר.
2. אלפי מסמכי נייר המתקבלים מידי שנה במשרד גורמים לנזק סביבתי מצטבר (הדפסה) ומחייבים את המשרד להגדיל את שטחי האחסון והשמירה על המסמכים.
3. רוב ספקי המשרד לא משולבים היום במערך הדיגיטציה.
4. לצוות הטכני של המשרד אין מידע בזמן אמת לגבי תעבורת הסחר האלקטרוני אצל המפעילים הקיימים.
5. אין קריטריונים ידועים וברורים לרמות השירות המוענקים לספקים.
6. אין הגדרת סוגי שירות ומחירון מוסכם ומחייב.

## 1. תנאים כלליים

### 1.0 כללי

### 1.1 הגדרות

להלן מונחים מרכזיים במסמך דרישות זה:

| # | המונח | הגדרה / הסבר |
| --- | --- | --- |
| 1 | הלקוח / המשרד | משרד הביטחון. |
| 2 | המגיש | ספק המשרד אשר מגיש מועמדותו לקבלת סיווג ספק מורשה קשר דיגיטלי מסחרי (להלן קד"ם) |
| 3 | המפעיל | ספק המשרד אשר עמד בכל הדרישות לסיווג קד"ם והוכר כספק מורשה לנושא קשר דיגיטלי מסחרי |
| 4 | ספקי המשרד | ארגונים וחברות המוכרים כספקי טובין ו/או שירותים למשהב"ט, אשר איתם מעוניין המשרד לנהל קשרי סחר אלקטרוני הכולל, בין היתר, העברת מסרים אלקטרוניים דו כיווניים.  ספקי המשרד יהיו לקוחות פוטנציאליים או לקוחות היעד של המפעיל/ים לצורך קבלת מגוון שירותים כמתואר במסך הדרישות הנ"ל. |
| 5 | תקופת הרשיון | כל התקופה אשר בה המגיש אשר הוכר כספק מורשה קד"ם והפך למפעיל מקיים קשר דיגיטאלי מול משרד הביטחון. |

### 1.2 התחייבויות ואישורים בגין הגשת המועמדות

המגיש יצרף לבקשתו את המסמכים והאישורים הנדרשים במסמך זה, לרבות נספחיו.

#### 1.2.0 כתב ערבות

כל רכיבי הפתרון המוצע (למעט תוכנה שתפותח במיוחד לצורך המערכת) הם בשירות ותחזוקה שוטפים. המגיש מתחייב לקיים השירות לספקי משרד הביטחון ולעמוד בכל תנאי מסמך זה לרבות העדכונים שיפורסמו מעת לעת למשך שלוש (3) שנים לפחות מיום אישור סיווגו כספק קד"ם. למען הבטחת השירות, יצרף המגיש לבקשתו ערבות בנקאית אוטונומית / כתב ערבות חברת ביטוח בלתי מותנית על סך 50000 ₪, כמצורף בנספח ז, אשר יעמוד בתוקפו למשך שלוש (3) שנים ויוארך מעת לעת ע"י המשרד כל עוד הסיווג תקף.

ככל שהספק הפר את תנאי הסיווג או לא מילא אחר הוראותיו, משהב"ט שומר לעצמו את הזכות לחילוט הערבות כולה או חלקה בהתאם לשיקול דעתו הבלעדי.

ככל שיבחר המשרד לחלט את הערבות כולה או חלקה, על המציע להשלים את הערבות בגובה הסכום שחולט באופן מידי.

אי ביצוע האמור מהווה הפרה של תנאי הסיווג היכול לגרור לחילוט כל סכום הערבות ו/או ביטול או השהיית הסיווג של הספק, הכל בהתאם לשיקול דעתו הבלעדי של המשרד.

יובהר, כי היה והחליט משרד הביטחון לחלט את העברות כולה או חלקה, לא יהיו לספק כל טענה ו/או תביעה כנגד משרד הביטחון בשל כך.

### 1.3 זכויות משהב"ט

#### 1.3.0 סיור במתקני המגיש

על פי שיקול דעת המשרד יאפשר המגיש לערוך סיור במתקני אירוח השרתים שלו, מוקד השירות שהוא מפעיל וכו'. המגיש מתחייב להיענות לבקשות האמורות של המשרד וכן למסור הבהרות, מידע ותשובות לשאלות שיוצגו בפניו על ידי המשרד וייעתר לבקשה של המשרד או מי מטעמו לבקר במתקניו ובחצריו של המגיש.

### 1.4 תנאים מקדמיים להגשת בקשה להכרה כספק מוכר לעניין קד"ם

#### 1.4.0 המעמד המשפטי

המגיש הוא ספק מוכר של משהב"ט

#### 1.4.1 נסיון רלוונטי והיקף פעילות המגיש

1. המגיש מספק שירותי מיסור לפחות ל- 1000 לקוחות פעילים המחוברים לשירותיו ומעבירים באמצעותו מסרים באופן שוטף במהלך 12 החודשים האחרונים נכון למועד ההגשה (להלן "התקופה הקובעת").
2. המגיש מזרים בין לקוחותיו לפחות 20000 מסרים ביום בתקופה הקובעת.
3. המגיש מזרים לפחות 1 GB נפח תעבורה ביום בתקופה הקובעת..
4. למגיש יש יכולת מובנית ופעילה להעברת מסרים בנפחים של לפחות 2 Gb.
5. למגיש יכולת מובנית ופעילה להעברת מסרים בכמות יומית כוללת של לפחות 100000 מסרים בתקופה הקובעת..
6. למגיש יש ניסיון מוכח של לפחות ארבע (4) שנים בכלל השירותים הנדרשים כמפורט בסעיף 2.3.0 להלן.
7. למגיש יש תוכנת לקוח הניתנת להתקנה על שרתי המשרד, ללא תלות בהתקנה ותחזוקה של מאגר נתונים חיצוני.
8. למערכות המגיש פתרון DRP שיאפשר זמינות מלאה כנדרש בסעיף 2.19 אבטחת המידע. המשרד רואה בנושא הזמינות עוגן עיקרי של המערכת.
9. למגיש יש במערכותיו האוטומטיות סביבה מלאה לביצוע בדיקות אשר אינה חופפת לסביבת הייצור. האמור לעיל נכון הן למערכות ה-B2B והן למערכות הפורטל.
10. למגיש יש שרת כספות של cyberark או כלים המאפשרים דחיפה ומשיכה של קבצים משרת\ים כאלה באתר\ים מרוחק\ים.
11. למגיש יש ניסיון בהפעלת מוקד שירות לקוחות בתחומי B2B ופורטל עסקי של שנתיים לפחות.

#### 1.4.2 עמידה בדרישות החוק והרגולציה

1. המגיש יתכנן את המערכת, ויתחזק את פעולתה, תוך עמידה בדרישות המובעות בהוראות כל דין, לרבות החוקים והרגולציות הבאים:
2. הוראות חוק הגנת הפרטיות ותקנות רישום מאגרי מידע וכל דין הקשור אליהם.
3. הוראות רגולציית אבטחת פרטי מחזיקי כרטיסי האשראי PCI-DSS.
4. מבלי לגרוע מהאמור לעיל, המערכת תעמוד לעניין אבטחת מידע בכל הוראת דין רלבנטית, כפי שתחול מעת לעת.
5. המגיש מתחייב לעמוד בדרישות המובעות בהוראות אלו, ובכל עדכון או שינוי שלהם, עפ"י המועדים אשר יהיו נקובים בתקנות או החוקים החדשים עם פרסומם.
6. במידה והמגיש גובה תשלומים מהספקים באמצעות כרטיסי אשראי יצהיר כי, מערכת גביית התשלומים מהספקים בכרטיסי אשראי עומדת בדרישות מועצת חברות כרטיסי האשראי (מועצת PCI) ודרישות חברות כרטיסי האשראי, כמצורף בנספח ו.
7. למגיש יש תו תקן ISO9001:2008

#### 1.4.3 מסמכים ואישורים

1. על המגיש לספק למשרד הביטחון את כל המסמכים והאישורים הנדרשים להוכחת עמידתו בתנאים המפורטים לעיל כמפורט בסעיף ב דלהלן. יודגש כי המגיש מתחייב להעביר למשרד הבהרות, מסמכים ואישורים נוספים, אשר לפי שיקול דעתו הבלעדי של המשרד נדרשים על מנת להוכיח את עמידתו בתנאים המפורטים במסמך זה.
2. רשימת המסמכים הנדרשים:
   * + 1. מסמך אישור כללי (נספח ב)
       2. מסמך אישור תהליכים (נספח ג)
       3. מסמך אישור תוכנת סוכן
       4. מסמך פירוט לסעיף 3.2 בו יתאר את המענה הקיים אצלו בכל תת סעיף בו התבקש לפרט.
       5. מסמך אישור תוכנת סוכן (נספח ד).
       6. טבלת דרישות אבטחת מידע (קובץ אקסל) וכל הפירוטים הנדרשים במסגרתה כולל אישורי אבטחת מידע מסוקר חיצוני מוסמך CI (נספח ה)
       7. תצהיר PCI-DSS (נספח ו)
       8. כתב ערבות (נספח ז)

### 1.5 סיווג ספק מורשה קד"ם

#### 1.5.0 ביטול סיווג

למשרד שמורה הזכות, בהתאם לשיקול דעתו הבלעדי לבטל את סיווגו של ספק מורשה קד"ם, בשל הפרה של הוראות וכללי מסמך זה, וזאת תוך מתן הודעה מראש בכתב לספק לפחות 30 יום. היה ולדעת המשרד המדובר בנושא ביטחוני, שמורה למשרד הזכות לבטל את סיווגו של הספק באופן מיידי וללא התראה מראש..

#### 1.5.1 שינוי תנאי הדרישות לסיווג קד"ם

למשרד שמורה הזכות, בהתאם לשיקול דעתו הבלעדי, לשנות את התנאים לקבלת סיווג ספק מורשה קד"ם, על פי צרכיו, וזאת תוך מתן הודעה בכתב לספק מראש ובפרק זמן סביר אשר יצויין בהודעה כאמור, ואולם במקרה של נימוק ביטחוני אף ללא צורך בהתראה מראש.

#### 1.5.2 תנאי חובה לקבלת הסיווג

לאחר כי הוכיח המגיש שעמד בכל התנאים המפורטים במסמך זה , תנאי חובה על מנת לקבל את הסיווג הינו ביצוע מבחני קבלה לממשקים הממוכנים המפורטים בסעיף 2.5 מול המערכות בסביבת הטסט של משהב"ט. (ראה נספח כא הפרט את תהליך קבלת הסיווג)

### 1.6 הגינות עיסקית

* + 1. יושרה והגינות עיסקית

על המפעיל לשמור על שוק תחרותי ולנהוג ביושרה והגינות עיסקית כלפי ספקי המשרד וכלפי מפעילים מורשים אחרים של המשרד.

למען הסר ספק, אי עמידה בסעיף זה כמוהו כאי עמידה בכל תנאי אחר במסמך התנאים. אי לכך ייתכן כי יופעלו בגין הפרתו הגנות כפי שבאות לידי ביטוי בסעיפים 1.2.0 ו-1.5.0.

## 2. יישום –דרישות עיסקיות

### 2.0 כללי

בין משרד הביטחון לבין ספקי המשרד מנוהלת מערכת תהליכים של שרשרת אספקה אשר תומכת בתהליכי הרכש של המשרד. משרד הביטחון מבקש להשיג דיגיטציה מלאה של שרשרת האספקה, מתוך הכרה בתכונות היעילות, הדיוק והחיסכון שמהלך כזה יביא. השגת יעד זה כרוך בתהליך מורכב של קישור אלפי ספקים של המשרד למערכות המשרד. באמצעות חיבורי תקשורת, התאמות פורמטים, התמודדות עם סוגיות אבטחת מידע והקמת צוותים ייעודיים להספקת שירותי הדרכה, תמיכה ועוד.

המשרד מכיר בערך המוסף של חברות אשר התמחותן בתיווך דיגיטלי והספקת שירותים נלווים להשלמת תהליכי הסחר האלקטרוני בין המשרד לספקיו, ומעוניין למסד ולהרחיב את השירות הקיים באופן שיענה על הדרישות המפורטות במסמך זה.

### 2.1 מאפיינים כלליים

#### 2.1.0 אופי מערכת המגיש וסוגה

המערכת צריכה להיות מערכת תפעולית מבוססת תהליכים, המשמשת כ HUB מרכזי המקשר ומגשר בין מערכות משהב"ט לבין ספקיו, בהעברת תשדורות המהוות את אבני הבניין של תהליכי שרשרת האספקה, באמצעים ממוכנים.

המערכת צריכה להיות מערכת בניית תהליכים (business process management) ומערכת קישוריות (enterprise service bus) אשר ביכולתה לתפור תהליכים custom made ולהתקשר ללקוח בצורות ואופנים שונים.

מכיון שמדובר במערכות אשר תומכות במערכות מבצעיות של המשרד ואשר זמינותם הוא חלק ניכר מאמינותם, המערכות צריכות להיות מנוטרות באופן אוטומטי ולהתריע בזמן אמת על תקלות שעלולות לפגוע ברמות השרות הנדרשות מהן.

מכיוון שהמערכות הינן מערכת "דיוור", על המערכות לדעת בכל רגע נתון היכן ומה קרה ל"חבילה" בודדת בדרך, ולהתריע לעיניים הנכונות בכל מקרה של תקלה.

על המערכות לשמור על מידור בין הספקים של המשרד ובין נתונים של המשרד לבין לקוחותיה האחרים של המגיש.

לצורך בדיקת עמידת המגיש בתנאים האמורים מסכים המגיש לביקור המשרד או מי מטעמו כאמור בסעיף 1.3.0.

#### 2.1.1 אילוצים

מערכת הסחר האלקטרוני נתונה למגבלות רגולטריות מעצם העובדה שתהליכי שרשרת האספקה כוללים שידור של חשבוניות מס. על המגיש לשמור באופן שוטף על תאימות המערכת לשינויים שעשויים להידרש מעת לעת על ידי המחוקק, רשויות המס וגורמי הרגולציה.

על המערכת להתאים עצמה למגבלות הטכנולוגיות שמעמידים ספקי המשרד בבואם להתחבר למערכת.

#### 2.1.2 מילון מונחים

|  |  |
| --- | --- |
| מונח | הגדרה |
| יום עבודה\עסקים | כהגדרתו בחוק שעות עבודה ומנוחה. |
| מסר מיידי | נתונים עיסקיים של המסר אשר ניתנים לאיחזור ממאגר הנתונים בשליפה רגילה |
| מסר ארכיון | נתונים עיסקיים ארוזים בקובץ ארכיון, אשר על מנת לצפות בהם יש לבצע תהליך של איחזור מקבצים וטעינה למאגר הנתונים. |

### 2.2 תיחום חיצוני

#### 2.2.0 תיחום כללי

ראה תרשים מודל סביבה בנספח א.

### 2.3 תיחום פנימי

#### 2.3.0 ארכיטקטורה ותיאור כללי של המערכת הנדרשת

1. ליבת המערכת נדרשת להיות תשתית מיסור של המגיש המהווה פלטפורמה ליישום תהליכי העברה של מסרים, לרבות התקשרות בפרוטוקולים שונים למערכות שונות, התחברות ל-agent-ים של המגיש ויכולת לספק תהליך מובנה ומנוטר של העברת מסרים וביצוע טרנספורמציות ממבנה למבנה, ואלידציות ולוגיקות תהליכיות אחרות. תשתית זו אמורה לעמוד בהיקפי עבודה גדולים.
2. מעל תשתית זו נדרשת שכבת שירותים: פורטל ו-B2B. שירותים אלה יינתנו ישירות לספקים. התשתית מחוייבת בשכבת ניטור שמורכבת משתי תתי שכבות. תת שכבה הנמוכה הינה ניטור תשתיתי – ניטורים בסיסיים של חיות המערכת, שרידות שרתים, ביצועים וחומרה וכן ניטורי בסיס על נפילות מסרים, תקיעת תורים וכן הלאה. תת השכבה הגבוהה הינה ניטור עיסקי – תגובה לאירועים חיוביים ושליליים כאחד כפונקציה של סוג התנועה, הערכים העיסקיים המופיעים בתנועה בודדת וכו'.

**אינדקס שירותים כללי נדרש.**

| סעיף | שם | הערות |
| --- | --- | --- |
| 2.3.1 | שירות מיסור B2B |  |
| 2.3.2 | שירות פורטל |  |
| 2.3.4 | שירותי ניטור עיסקי |  |
| 2.3.5 | שירותי שליפת מסרים ישנים |  |
| 2.3.6 | שירות הכנסת ספק חדש ומעבר ספק ממפעיל למפעיל |  |
|  |  |  |

#### 2.3.1 שירות מיסור B2B

שירות מיחשובי אשר מאפשר לספקים בעלי מערכות מיחשוביות המסוגלות ומעוניינות בכך לקלוט ולשדר באופן אוטומטי מסרים אל וממערכות המיחשוב של משהב"ט. השירות יספק יכולות טרנספורמציה על מנת להתאים את שפת המסר של השולח לשפת המסר של המקבל.

נדרש שהשירות יספק יכולות תהליכיות על מסרים: ניתוב על בסיס שם קובץ, ניתוב על בסיס ערכים עיסקיים בתוכן המסר, פיצול מסרים לכמה יעדים, מניעת זרימת מסר על בסיס ערכים עיסקיים מתוכן המסר ו\או על בסיס שם קובץ.

נדרש שהשירות יספק יכולות קישוריות על מסרים: התקשרות לצד ג' בפרוטוקולים שונים, עבודה מול ה-agent-ים של המגיש במקרה שלצד ג' חסרות יכולות קישוריות. יכולות אשר מהוות תנאי סף הינן יכולת עבודה מול FTP ויכולת עבודה מול כספות של cyberark.

כמו כן נדרשת יכולת שליחה חוזרת אגרגטיבית (על בסיס סוג מסר ספציפי ותאריך התחלה ותאריך סיום ו\או סטטוס).

נדרשת יכולת עבודה מול מבני מסרים בלפחות שלושת הפורמטים הבאים: XSD,WSDL,WCF.

נדרשת יכולת לבצע וולידציה על סכימות אילו.

נדרשת יכולת לאסוף נתונים עיסקיים מתוך המסרים לתוך מאגר נתונים מרכזי, ממנו ניתן יהיה להפיק מסכי שאילתא ודוחות לספקים השונים.

לצורך בדיקת עמידת המגיש בתנאים האמורים מסכים המגיש לביקור המשרד או מי מטעמו כאמור בסעיף 1.3.0.

#### 2.3.2 שירות פורטל

נדרש שירות אינטרנטי שיאפשר לספקים להתחבר למערכות המגיש ולצפות במצב התנועות של תהליכים שנוגעים לספק מול משהב"ט. השירות אמור לאפשר לספקי המשרד לבצע בקרה אחר תנועות אחרונות, לבצע חיפושים, להזין נתונים שיתורגמו למסרים אשר יישלחו למשהב"ט, לבצע תיקון ושליחה חוזרת של מסרים, להעלות מסמכים אלקטרוניים ולשדכם למסרי מקור.

על המשתמש מטעם ספק המשרד המחובר לשירות להיות מסוגל:

1. לראות את כל סוגי התנועות שהתבצעו מול משהב"ט, וסטטוס הביצוע שלהם.
2. לראות קישור בין יישות מובילה\ראשית (הזמנה) לבין כל התנועות הקשורות אליה.
3. לבצע חיפוש לתנועות על בסיס מאפיינים עיסקיים.
4. להקליד נתונים של חשבונית שיאומתו מול נתוני הזמנה ובסיום מוצלח לשלוח מסר חשבונית למשהב"ט.
5. יכולת להעלות מסמכים ולקשר אותם למסר שנשלח למשהב"ט.
6. להפיק פלט ויזה ממסך צפייה בפקודת עבודה.

אפשרות שליפת מידע ומסמכים עבור מסרים ישנים

נדרשת יכולת לבצע חיפושים מיידיים, ללא צורך באיחזור מארכיון, על מסרים שנשלחו על ידי המשרד וספקיו כחצי שנה אחורה בכל יום נתון.

הדרשת יכולת מידור של כל ספק המשרד לאינפורמציה הרלוונטית אליו בלבד.

נדרשת אפשרות למשרד הביטחון לקבל עד חמישה משתמשים אדמיניסטרטיביים, על פי דרישה, אשר יהיו להם היכולת לראות את נתוני כל ספקי המשרד.

#### 2.3.3 שירותי ניטור עיסקי

נדרשת יכולת שליחת התראות ומסרים אוטומטיים, כפי שיוגדרו ע"י המשרד, בתגובה לאירועים כגון תקלה, אי העברת מסר, timeout למסר תקוע וכו'.

לצורך בדיקת עמידת המגיש בתנאים האמורים מסכים המגיש לביקור המשרד או מי מטעמו כאמור בסעיף 1.3.0.

#### 2.3.4 שירותי שליפת מסרים ישנים

על המגיש קיימת החובה לא למחוק מסרים אשר אינם בסטטוס סופי על פי האיפיון של הסטטוסים הספציפי לכל מסר.

מסרים שבסטטוס סופי יוחזקו עבור כל ספק כשנה אחורה. כאשר מדובר בפקודות אספקה או עבודה אשר אליהן קשורים מסרים נוספים בשרשרת האספקה, יש להתייחס לתאריך המסר האחרון הקשור כתאריך הקובע.

המגיש יאפשר איחזור ושליפת מסרים ומסמכים הקשורים לכלל המסרים האלה.

כל ספק יוכל לאחזר ולשלוף אך ורק מסרים הקשורים אליו.

צוותים טכניים של משהב"ט יוכלו לצפות במסרים של כל הספקים.

#### 2.3.5 שירות הכנסת ספק חדש ומעבר ספק ממפעיל למפעיל

שירות זה מטרתו הכנסת ספק חדש לשירותי המגיש. ספק חדש יכול להיות ספק שאין לו רקע בעבודה מול מפעיל בכלל ומיחשובית בפרט, או לחילופין ייתכן שמדובר בספק שהחליט לעבור ממפעיל קודם למפעיל נוכחי. על המגיש הקודם להבטיח מעבר בטוח של הספק על ידי עמידה בדרישות מינימום שונות.(ראה פירוט בסעיף 4.2.2)

#### 2.3.6 שירות לקוחות

על המגיש לאפשר שירות לקוחות לספקי המשרד על פי הסטנדרטים המקובלים בשוק ובהתאם לכללים המפורטים בסעיף 4.1.

### 2.4 ממשק משתמש

#### 2.4.0 כללי הנדסת אנוש

עבור ממשקי המשתמש המשרתים את הספקים ואת צוותי המשרד נדרשות פשטות הפעלה, וביצועים מהירים.

### 2.5 תהליכים

לצורך בדיקת עמידת המגיש בתנאים האמורים מסכים המגיש לביקור המשרד או מי מטעמו כאמור בסעיף 1.3.0. זאת עבור כל אחד מסעיפי המשנה של סעיף זה.

#### 2.5.0 רשימת תהליכים

1. תהליכי המיסור המפורטים מטה מהווים את המינימום הנדרש כתנאי סף.
2. המגיש יוסיף לבקשתו מסמך המאשר כי ביכולתו לספק התהליכים המפורטים, כמובא בנספח ג.
3. המגיש יידרש לעמוד בחובת ההוכחה של יישום התהליכים כתנאי לקבלת הסיווג בהתממשקות דיגטאלית מלאה מול משהב"ט בסביבת הניסוי. יהיה עליו להתממשק בתהליכים המפורטים בסעיפים 2.5.3 – 2.5.20. וכל זאת אך ורק לאחר עמידה בתנאי אבטחת המידע המפורטים בסעיף 3.2.

| סעיף | שם | הערות |
| --- | --- | --- |
| 2.5.1 | שמירת נתון סוג מערכת |  |
| 2.5.2 | ריבוי מספרי ספק לגורם עיסקי אחד |  |
| 2.5.3 | שליחת הזמנת רכש למפעיל |  |
| 2.5.4 | שליחת מסר מחירון מרק"ט\נתיבים |  |
| 2.5.5 | שליחת פקודת אספקה(פק"א) מרק"ט לספק |  |
| 2.5.6 | קבלת אישור לפקודת אספקה מרק"ט מהספק |  |
| 2.5.7 | קבלת תעודת משלוח מהספק |  |
| 2.5.8 | שליחת אישור על תעודת משלוח לספק |  |
| 2.5.9 | שליחת דיווח קבלה לספק |  |
| 2.5.10 | שליחת פקודת עבודה(פק"ע) לספק |  |
| 2.5.11 | קבלת אישור לפק"ע מהספק |  |
| 2.5.12 | קבלת גיליון שירות מהספק |  |
| 2.5.13 | קבלת נתוני GPS עבור גיליון שירות מהספק |  |
| 2.5.14 | שליחת אישור על גיליון שירות לספק |  |
| 2.5.15 | שליחת תחשיב לתשלום לספק |  |
| 2.5.16 | קבלת חשבונית לוגיסטית מהספק ע"ס הזמנת רכש |  |
| 2.5.17 | קבלת חשבונית לוגיסטית נתיבים מהספק |  |
| 2.5.18 | קבלת חשבונית לוגיסטית מרק"ט מהספק |  |
| 2.5.19 | שליחת סטאטוס חשבונית לספק |  |
| 2.5.20 | שליחת הודעת זיכוי לספק |  |
|  |  |  |
|  |  |  |

#### 2.5.1 שמירת נתון סוג מערכת.

בכל הטרנזקציות אשר בהן שומרים נתונים עיסקיים על מסרים יש לשמור נתון המעיד על סוג המערכת המעורבת במשהב"ט, לצורך חיתוכים במסכי הפעולה והחיפוש. לדוגמא: מרק"ט, נתיבים וכו'. בחלק מהמסרים סוג המסר עצמו מעיד על סוג המערכת ובחלק אחר שבו המסר הוא גנרי נתון עיסקי בתוכן המסר מעיד על כך.

נתון זה הינו נתון חשוב ביותר במערך ההפעלה של המסרים של משהב"ט. יידרש על ידי המגיש גם לציין, עבור מסרים גנריים שיוצאים מהמגיש לכיוון משהב"ט (לדוגמא: חשבונית), בשדה אחד או יותר את סוג המערכת.

#### 2.5.2 ריבוי מספרי ספק לגורם עיסקי אחד

סעיף זה רלוונטי בכל מקום במסמך זה בו יש התייחסות לספק בלשון יחיד.

תיתכן סיטואציה בה ספק מוכר של המשרד הבא בהתקשרות עם המפעיל הוא בעל יותר ממספר ספק אחד (ייתכן חברה בעלת ח.פ. אחד עם יותר ממספר ספק אחד או חברת אם וחברת בת כאשר חברת האם מבקשת לבצע את כל או חלק מהפעילות העיסקית של חברת הבת מול המערכות שלה).

אי לכך נדרש:

1. שירותי B2B : המגיש יאפשר יישום של ניתוב מסרים המתחשב בכך שייתכן שמספר מספרי ספק אמורים להיות מנותבים לגורם אחד.
2. שירותי פורטל : המגיש יאפשר אופציה לגורם אחד לראות את כל מספרי הספק הרלוונטיים אליו, ואך ורק אליו, בכל מסכי הפורטל המפורטים ברחבי המסמך הזה.

#### 2.5.3 שליחת הזמנת רכש למפעיל

|  |  |
| --- | --- |
|  | **שליחת הזמנת רכש למפעיל** |
| תיאור הנדרש | משהב"ט ישלח מסר הזמנה אשר מכיל נתונים על בסיסם ניתן יהיה לבצע בדיקות תאימות לחשבוניות הלוגיסטיות, מספרי שורות הפריטים בחשבונית יהיו זהים למספרי שורות ההזמנה.  אי לכך על המגיש לשמור את נתוני ההזמנה גם לצורכי הצגה וגם לצורכי בדיקת תאימות בין שורות הפריטים בהזמנה לשורות הפריטים בחשבונית הלוגיסטית.  יש לבדוק אם קיים כבר מספר הזמנה ולעדכן אחרת יש לבנות רשומה חדשה.  בכל שינוי של הזמנה יישלח מסר המכיל את ההזמנה המתוקנת (גירסאות). כלומר יצא שוב מסר הזמנה שמכיל תמונת מצב מלאה חדשה. בביטול של כל ההזמנה ייצא מסר הזמנה עם סימון מיוחד שמעיד על ביטולו.  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי קליטת ההזמנה, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע קליטה, יש להפעיל טרנזאקציית שליחת התראה.  שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS (על פי קביעה עם המשרד). ההתראה צריכה להכיל נתונים עסקיים נדרשים: מספר הזמנה ומספר מסר. |
| מסכי פעולה | 1. מסך צפייה לכל ספק להזמנות שלו |
| תדירות | עשרות – מאות ביום |
| שעות פעילות ממשק | 7-20 |
| שולח | משהב"ט |
| מקבל | המגיש |
| טיפול בשגיאות סיסטם | יש לשלוח התראה במייל למשהב"ט |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר | 1. איפיון מבנה המסר: ראה נספח ט 2. איפיון אלגוריתם שליחה לספקים מתווכים מקבלי המסר – נספח יא |

#### 2.5.4 שליחת מסר מחירון מרק"ט\נתיבים

|  |  |
| --- | --- |
|  | **שליחת מסר מחירון נתיבים** |
| תיאור הנדרש | לאחר יצירה או עידכון של הסכם מחירים יישלח לספק מסר מחירון שמכיל את נתוני המחירון המעודכן המלא. מחירון הוא חלק מההסכם, כאשר לכל הסכם יש ספק אחד או יותר שזכו בו וניתן לאפשר אך ורק לספקים אילו לצפות בו. המחירון הינו לצפייה בלבד, ואינו ניתן לשינוי על ידי גורמים מחוץ למשרד הביטחון.  במסר מחירון יופיע סוג המערכת אליו שייך(מרק"ט או נתיבים) |
| מסכי הפעולה | יש להציג לכל ספק את המחירון הרלוונטי אליו על פי הסכם המחירים הספציפי. |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | משהב"ט |
| מקבל | הספק |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר |  |

#### 2.5.5 שליחת פקודת אספקה(פק"א) מרק"ט לספק

|  |  |
| --- | --- |
|  | **שליחת פקודת אספקה(פק"א) מרק"ט לספק** |
| תיאור הנדרש | מסר ממערכת מרק"ט המכיל בקשה של משהב"ט לאספקה של טובין או שירות כלשהוא מספק המשרד.  מסר זה מהווה את הבסיס לכל שרשרת האספקה ומהווה יישות במערכת אשר מנוהלת על ידי סטטוסים המשתנים בהתאם ללוגיקה של המסרים שיוגדרו בהמשך.  עם קבלת הפקודה יש להקים יישות חדשה במערכת ולסמנה בסטטוס "התקבלה פקודה".  יש לאפשר אופציה לספק לקבל התראה מסוג של מייל או סמס או פקס.  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי קליטת ההזמנה, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע קליטה, יש להפעיל טרנזאקציית שליחת התראה למשהב"ט.  שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS (על פי קביעה עם המשרד). ההתראה צריכה להכיל נתונים עסקיים נדרשים: מספר פק"א, מספר מסר ומספר ספק. |
| מסכי פעולה | 1. מסך צפייה לכל ספק בפקודת האספקה שלו |
| תדירות | עשרות – מאות ביום |
| שעות פעילות ממשק | כל היום |
| שולח | משהב"ט |
| מקבל | הספק |
| טיפול בשגיאות סיסטם | יש לשלוח התראה במייל למשהב"ט |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר |  |

#### 2.5.6 קבלת אישור לפקודת אספקה מרק"ט מהספק

|  |  |
| --- | --- |
|  | **קבלת אישור לפקודת אספקה מרק"ט מהספק** |
| תיאור הנדרש | במערכת מרק"ט לאחר שיצאה פקודת האספקה לספק, על הספק לשלוח למשהב"ט אישור על קבלת הפקודה.  עם הגעת המסר, יש לשנות את הסטאטוס של הפקודה ל"אושר על ידי הספק", לשמור את תאריך, שעת האישור וזהות המאשר (אם מדובר במסך הפורטל), יש להיערך למצב של ריבוי אישורים על אותה פקודה אם היו שינויים בתוכן הפקודה ונשלחה יותר מפעם אחת לספק.  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי העברת האישור פק"א\פק"ע, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע העברה, יש להפעיל טרנזאקציית שליחת התראה.  שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS. ההתראה צריכה להכיל נתונים עסקיים נדרשים: על פי הסיכום בין הספק למפעיל. |
| תדירות | עשרות – מאות ביום |
| מסכי פעולה | 1. מסך הזנת אישור ספק לפקודת אספקה שיחולל את המסר למשהב"ט. |
| שעות פעילות ממשק | כל היום |
| שולח | הספק |
| מקבל | משהב"ט |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר |  |

#### 2.5.7 קבלת תעודת משלוח מהספק

|  |  |
| --- | --- |
|  | **קבלת תעודת משלוח מהספק** |
| תיאור הנדרש | במערכת מרק"ט תיתכן אפשרות של ריבוי תעודות משלוח לפקודת אספקה אחת. אי לכך יש לנהל סטטוסים על תעודות המישלוח. הסטטוס הראשון בעת שליחת תעודת המישלוח הינו "נשלח למשהב"ט".  יש לעדכן ב-DB את הנתונים המוזנים על ידי ספקי הפורטל או את הנתונים אשר מופיעים בקובץ הנשלח על ידי ספקי ה-B2B. יש להיערך לריבוי גרסאות של תעודות משלוח.  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי העברת גיליון השירות, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע העברה, יש להפעיל טרנזאקציית שליחת התראה לספק. שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS. ההתראה צריכה להכיל נתונים עסקיים נדרשים: על פי הסיכום בין הספק למפעיל.  כאשר הכמויות המצטברות עבור כל שורה בפקודה כפי שמשתקף מכל תעודות המישלוח שווה לזו המופיעה בפק"א יש לשנות את הסטטוס של הפק"א ל"סופקה". |
| מסכי פעולה | 1. מסך צפייה לכל ספק על התעודות הקשורות לפקודה ספציפית שלו. 2. מסך שיאפשר מבט על וביצוע חתכים על כל תעודות המישלוח (לדוגמא לפי תאריך, לפי מערכת וכו') ששיכות לספק. 3. מסך הזנת נתונים לתעודת משלוח לצורך חילול המסר למשהב"ט. |
| תדירות | עשרות – מאות ביום |
| שעות פעילות ממשק | כל היום |
| שולח | הספק |
| מקבל | משהב"ט |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר |  |

#### 2.5.8 שליחת אישור על תעודת משלוח לספק

|  |  |
| --- | --- |
|  | **שליחת אישור על תעודת משלוח לספק** |
| תיאור הנדרש | במערכת מרק"ט לאחר שהגיעה תעודת המשלוח מבצעות כל הבדיקות הנדרשות מול נתוני ההזמנה והנתונים שסופקו בתעודת המשלוח. התוצר הוא מסר אישור על תעודת המשלוח לספק. במידה ומסר האישור מכיל קוד שגיאה 9 (שדה "קוד תקינות מסר תעודת משלוח), יש לשנות סטטוס תעודת המישלוח ל"תעודת המשלוח במשהב"ט תקינה" אחרת (קוד 5,4) יש לשנות סטטוס תעודת המישלוח ל"תעודת המשלוח במשהב"ט שגוייה". |
| מסכי פעולה | מסך צפייה בפירוט השגויים (סגמנט HeadErrLines) |
| תדירות | עשרות – מאות ביום |
| שעות פעילות ממשק | כל היום |
| שולח | הספק |
| מקבל | משהב"ט |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר |  |

#### 2.5.9 שליחת דיווח קבלה לספק

|  |  |
| --- | --- |
|  | **שליחת דיווח קבלה לספק** |
| תיאור הנדרש | נתוני הדיווח שבוצעו ע"י המשתמש במערכת מרק"ט ע"ס התעודת משלוח ונתוני הפק"א יוצרים מסר דיווח קבלה שעל בסיסו יכול הספק לבנות חשבונית שתאושר.  יש לשנות סטטוס תעודת המישלוח ל"התקבל דיווח קבלה".  יש להיערך לאפשרות שליחה חוזרת של הדיווחים לצורך עדכון שינויים (גרסאות). |
| מסכי הפעולה | מסך פערים בין התעודת משלוח שהספק שלח לבין דיווח הקבלה שהתקבל ממרק"ט |
| תדירות | עשרות – מאות ביום |
| שעות פעילות ממשק | ריצה יומית בשעה 19:00 |
| שולח | משהב"ט |
| מקבל | הספק |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר |  |

#### 2.5.10 שליחת פקודת עבודה(פק"ע) לספק

|  |  |
| --- | --- |
|  | **שליחת פקודת עבודה(פק"ע) נתיבים לספק** |
| תיאור הנדרש | מסר ממערכת נתיבים המכיל בקשה של משהב"ט לאספקה של טובין או שירות כלשהוא מספק המשרד.  מסר זה מהווה את הבסיס לכל שרשרת האספקה ומהווה יישות במערכת אשר מנוהלת על ידי סטטוסים המשתנים בהתאם ללוגיקה של המסרים שיוגדרו בהמשך.  לספקים שמקבלים מסרים ישירות למערכות שלהן יש להעביר את המסר. בנוסף יש לטפל בפורטל הספקים כך שעם קבלת הפקודה יש להקים יישות חדשה במערכת ולסמנה בסטטוס "התקבלה פקודה".  המסר יגיע עם קובץ PDF המכיל את תדפיס הפקודה, כאשר קובץ ה-PDF בפורמט base64. תדפיס זה יש לאפשר לספק לצפות בו ולהדפיסו.  יש לאפשר אופציה לספק לקבל התראה מסוג של מייל או סמס או פקס.  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי קליטת ההזמנה, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע קליטה, יש להפעיל טרנזאקציית שליחת התראה למשהב"ט.  שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS (על פי קביעה עם המשרד). ההתראה צריכה להכיל נתונים עסקיים נדרשים: מספר פק"א, מספר מסר ומספר ספק.  קבלת ההחלטה לגבי היעד של המסר: ראה נספח יא |
| מסכי הפעולה | 1. מסך צפייה לכל ספק לפקודות העבודה שלו. |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | משהב"ט |
| מקבל | הספק |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר | 1. איפיון מבנה המסר: ראה נספח י 2. איפיון אלגוריתם שליחה לספקים מתווכים מקבלי המסר – נספח יא |

#### 2.5.11 קבלת אישור לפק"ע מהספק

|  |  |
| --- | --- |
|  | **קבלת אישור לפק"ע מהספק** |
| תיאור הנדרש | במערכת נתיבים לאחר שיצאה פקודת האספקה לספק, על הספק לשלוח למשהב"ט אישור על קבלת הפקודה.  עם הגעת המסר, יש לשנות את הסטאטוס של הפקודה ל"אושר על ידי הספק", לשמור את תאריך, שעת האישור וזהות המאשר (אם מדובר במסך הפורטל), יש להיערך למצב של ריבוי אישורים על אותה פקודה אם היו שינויים בתוכן הפקודה ונשלחה יותר מפעם אחת לספק.  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי העברת האישור, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע העברה, יש להפעיל טרנזאקציית שליחת התראה.  שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS. ההתראה צריכה להכיל נתונים עסקיים נדרשים: על פי הסיכום בין הספק למפעיל. |
| מסכי הפעולה | 1. מסך הזנת נתוני אישור פק"ע לצורך חילול המסר למשהב"ט. |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | משהב"ט |
| מקבל | הספק |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר | ראה נספח יא |

#### 2.5.12 קבלת גיליון שירות מהספק

|  |  |
| --- | --- |
|  | **קבלת גיליון שירות מהספק** |
| תיאור הנדרש | במערכת נתיבים לאחר שהספק סיפק את השירות עליו לשלוח למשהב"ט מסר גיליון שירות. בניגוד למרק"ט שבה לכל פק"א ייתכנו תעודות מישלוח רבות, בפק"ע יש אפשרות רק לגיליון שירות אחד. אי לכך לא ינוהל סטטוס פר גיליון שירות אלא רק הסטטוס של הפקודה. יש 2 סוגי גיליונות שירות, האחד שמחייב נתוני GPS ואחד שלא מחייב נתוני GPS (על פי המצויין בשדה "דגל נדרשים נתוני GPS" בפק"ע). כאשר לא מחוייב נתוני GPS יש לשלוח למשהב"ט מיידית ולשנות סטטוס הפקודה ל"נשלח גיליון שירות". כאשר מחוייבים נתוני GPS ועדיין לא התקבלו יש לשנות סטטוס הפקודה ל"ממתין לנתוני GPS" ולא לשלוח למשהב"ט את הגיליון.  יש להיערך לאפשרות של שליחה חוזרת של הגיליונות לצורכי עדכון שינויים (גרסאות).  תיתכן דרישה לצרף מסמכים סרוקים למסר.  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי העברת הגיליון למשהב"ט, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע העברה, יש להפעיל טרנזאקציית שליחת התראה לספק.  שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS. ההתראה צריכה להכיל נתונים עסקיים נדרשים: על פי הסיכום בין הספק למפעיל. |
| מסכי הפעולה | 1. מסך צפייה לכל פקודה לגיליון השירות שלה. 2. מסך הזנת נתוני גיליון שירות לצורך חילול המסר למשהב"ט. |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | הספק |
| מקבל | משהב"ט |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר | ראה נספח יב |

#### 2.5.13 קבלת נתוני GPS עבור גיליון שירות מהספק

|  |  |
| --- | --- |
|  | **קבלת גיליון שירות מהספק** |
| תיאור הנדרש | במערכת נתיבים לאחר שהספק סיפק את השירות עליו לשלוח למשהב"ט מסר גיליון שירות. במקרים שבהם בפקודת העבודה צויין שיש לצרף נתוני GPS אין לשלוח את גיליון השירות ללא קבלת נתוני ה-GPS מהספק. כלומר יש לשלוח גיליון שירות כשמיד לאחריו את מסר נתוני GPS. רק לאחר שליחת גיליון השירות + נתוני ה-GPS יש לשנות את סטטוס הפקודה ל"נשלח גיליון שירות".  יש להיערך לאפשרות של שליחה חוזרת.  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי העברת נתוני ה-GPS, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע העברה, יש להפעיל טרנזאקציית שליחת התראה לספק. שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS. ההתראה צריכה להכיל נתונים עסקיים נדרשים: על פי הסיכום בין הספק למפעיל. |
| מסכי הפעולה | 1. לאפשר במסך גיליון שירות לצפות בקובץ ה-GPS המצורף. 2. מסך העלאת קובץ GPS על ידי הספק. |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | הספק |
| מקבל | משהב"ט |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר |  |

#### 2.5.14 שליחת אישור על גיליון שירות לספק

|  |  |
| --- | --- |
|  | **שליחת אישור על גיליון שירות לספק** |
| תיאור הנדרש | לאחר שנקלט גיליון השירות במערכת נתיבים נשלח מיידית מסר אישור על גיליון השירות לספק. באם מדובר בספק שמקבל את המסר ישירות למערכותיו יש לשלוח אליו ובנוסף:  עם הגעתו למפעיל יש לשנות את הסטאטוס של הפקודה ל"גיליון שירות נקלט" בפורטל הספקים של המפעיל. |
| מסכי הפעולה |  |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | הספק |
| מקבל | משהב"ט |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר |  |

#### 2.5.15 שליחת תחשיב לתשלום לספק

|  |  |
| --- | --- |
|  | **שליחת תחשיב לתשלום לספק** |
| תיאור הנדרש | מערכות נתיבים מבצעת את כל הבדיקות הנדרשות לצורך התשלום לספק על בסיס נתוני ההזמנה והנתונים שסופקו בגיליון השירות. כתוצאה מהבדיקות והאישור (אוטומאטי או ידני) יוצא מסר תחשיב לתשלום שעל בסיסו יכול הספק לבנות חשבונית שתאושר.  יש לשנות את סטטוס הפקודה ל"התקבל תחשיב לתשלום".  יש להיערך לאפשרות שליחה חוזרת של התחשיבים לתשלום לצורך עדכון שינויים (גרסאות).  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי שליחת התחשיב לספק, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע קליטה, יש להפעיל טרנזאקציית שליחת התראה למשהב"ט.  שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS (על פי קביעה עם המשרד). ההתראה צריכה להכיל נתונים עסקיים נדרשים: מספר פק"ע, מספר תחשיב לתשלום, מספר מסר, מספר ספק ותאריך.  קבלת ההחלטה לגבי היעד של המסר: ראה נספח יא |
| מסכי הפעולה | 1. מסך צפייה לכל ספק בתחשיבם לתשלום שלו. |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | משהב"ט |
| מקבל | הספק |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר | 1. איפיון מבנה המסר: ראה נספח יג 2. איפיון אלגוריתם שליחה לספקים מתווכים מקבלי המסר – נספח יא |

#### 2.5.16 קבלת חשבונית לוגיסטית מהספק ע"ס הזמנת רכש

|  |  |
| --- | --- |
|  | **קבלת חשבונית לוגיסטית מהספק ע"ס הזמנת רכש** |
| תיאור הנדרש | יש למנוע העברת חשבונית שאינה מכילה שורות פריט (שמכילה רק סגמנט של כותרת).  יש למנוע העברת החשבונית באם לא ניתן אישור ספק להזמנת הרכש. זאת בהתבסס על שדה ZZVNDACKNLDT במסר ההזמנה (ראה מסמך 4 – ממשק הזמנה יוצא למפעילים). אם שדה זה ריק המשמעות הינה שהספק לא אישר את ההזמנה ואי לכך יש למנוע את שליחתה של החשבונית למשרד הביטחון.  יש למנוע העברת חשבונית שתאריך החשבונית עתידי מיום שליחתה.  מסר חשבונית לוגיסטית על סמך הזמנת רכש, מתחלקת לשני סוגים בעלי אותו מבנה. סוג אחד הינו חשבונית בסיס (RE) והסוג השני הינה התייקרות (ZY). יש לבדוק שמספרי שורות הפריטים בחשבונית זהים למספרי שורות הפריטים בהזמנה.  אם החשבונית תואמת את נתוני ההזמנה ונשלחה בהצלחה למשהב"ט יש לשנות סטאטוס חשבונית ל"נשלחה חשבונית".  אם החשבונית אינה תואמת יש לשנות סטאטוס חשבונית ל"נכשלה בבדיקות תאימות" ולשלוח לספק התראה על כך.  במקרה של חשבונית בסיס יש למנוע הזנת נתוני השדות: חשבונית בסיס בסימוכין, תאריך חשבונית בסיס בסימוכין. ובמקרה של חשבונית התייקרות יש לחייב הזנת הנתונים בשדות הללו.  בתהליך זה יובאו בעתיד דרישות של הצמדת מסמכים סרוקים (תעודות משלוח וגיליונות שירות) שנלווים למסר החשבונית.  יש להיערך לשליחה חוזרת של חשבונית לצורך עדכון שינויים (גרסאות).  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי העברת החשבונית, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע העברה, יש להפעיל טרנזאקציית שליחת התראה.  שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS. |
| מסכי הפעולה | 1. מסך צפייה לכל ספק בחשבוניות שלו. 2. מסך הזנת נתוני חשבונית לצורך חילול המסר למשהב"ט. |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | הספק |
| מקבל | משהב"ט |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר | ראה נספח יד |

#### 2.5.17 קבלת חשבונית לוגיסטית נתיבים מהספק

|  |  |
| --- | --- |
|  | **קבלת חשבונית לוגיסטית נתיבים מהספק** |
| תיאור הנדרש | יש למנוע העברת חשבונית שאינה מכילה שורות פריט (שמכילה רק סגמנט של כותרת).  יש למנוע העברת חשבונית שתאריך החשבונית עתידי מיום שליחתה.  מסר חשבונית לוגיסטית נתיבים, תישלח על סמך גיליון שירות  עבור חשבוניות של מערכת נתיבים\מרק"ט החשבונית חייבת להיות תואמת לתחשיב לתשלום שהתקבל ממשהב"ט.  אם החשבונית תואמת את נתוני התחשיב לתשלום ונשלחה בהצלחה למשהב"ט יש לשנות סטאטוס חשבונית ל"נשלחה חשבונית".  אם החשבונית אינה תואמת יש לשנות סטאטוס חשבונית ל"נכשלה בבדיקות תאימות" ולשלוח לספק התראה על כך.  בתהליך זה ייתכנו דרישות של הצמדת מסמכים סרוקים למסר החשבונית.  יש להיערך לשליחה חוזרת של חשבונית לצורך עדכון שינויים (גרסאות).  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי העברת החשבונית, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע העברה, יש להפעיל טרנזאקציית שליחת התראה.  שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS. |
| מסכי הפעולה | 1. מסך צפייה לכל ספק בחשבוניות שלו. 2. מסך הזנת נתוני חשבונית לצורך חילול המסר למשהב"ט. |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | הספק |
| מקבל | משהב"ט |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר | ראה נספח טו |

#### 2.5.18 קבלת חשבונית לוגיסטית מרק"ט מהספק

|  |  |
| --- | --- |
|  | **קבלת חשבונית לוגיסטית נתיבים מהספק** |
| תיאור הנדרש | יש למנוע העברת חשבונית שאינה מכילה שורות פריט (שמכילה רק סגמנט של כותרת).  יש למנוע העברת חשבונית שתאריך החשבונית עתידי מיום שליחתה.  מסר חשבונית לוגיסטית מרק"ט, תישלח על סמך גיליון שירות  עבור חשבוניות של מערכת נתיבים\מרק"ט החשבונית חייבת להיות תואמת לתחשיב לתשלום שהתקבל ממשהב"ט.  אם החשבונית תואמת את נתוני התחשיב לתשלום ונשלחה בהצלחה למשהב"ט יש לשנות סטאטוס חשבונית ל"נשלחה חשבונית".  אם החשבונית אינה תואמת יש לשנות סטאטוס חשבונית ל"נכשלה בבדיקות תאימות" ולשלוח לספק התראה על כך.  בתהליך זה ייתכנו דרישות של הצמדת מסמכים סרוקים למסר החשבונית.  יש להיערך לשליחה חוזרת של חשבונית לצורך עדכון שינויים (גרסאות).  בכל מקרה שבו במערכות המגיש עולה שגיאה או סיטואציה שגורמת לאי העברת החשבונית, למעט אם נדרש באופן מיוחד על ידי משהב"ט למנוע העברה, יש להפעיל טרנזאקציית שליחת התראה.  שליחת ההתראה יכולה להתבקש בכל אחד מהאופנים הבאים: שליחת קובץ איתות, שליחת מייל או שליחת SMS. |
| מסכי הפעולה | 1. מסך צפייה לכל ספק בחשבוניות שלו. 2. מסך הזנת נתוני חשבונית לצורך חילול המסר למשהב"ט. |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | הספק |
| מקבל | משהב"ט |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר |  |

#### 2.5.19 שליחת סטאטוס חשבונית לספק

|  |  |
| --- | --- |
|  | **שליחת סטאטוס חשבונית לספק** |
| תיאור הנדרש | המערכות הפיננסיות של משהב"ט מדווחות פעם ביום על שינויים בסטאטוס החשבונית בסבב האישורים במשהב"ט. אם התבצע שינוי בסטאטוס של חשבונית כלשהיא ייצא בסוף אותו יום מסר המעיד על השינוי שבוצע בחשבונית. על המגיש להעביר לספק את הנתונים במקרה של ספק שמקבל את המסרים ישירות למערכותיו וגם להציג את הנתונים בפורטל הספקים שלו.  יש להיערך לריבוי מסרים פר חשבונית לצורך הצגת רצף סטאטוסים.  יש לשנות את סטאטוס החשבונית על פי הסטאטוס הרשום במסר בהתאם לטבלה בסעיף 1.2.10.2.  **במידה והגיע סטטוס התקבל\נקלט ממשהב"ט יש לחסום את האפשרות של הספק לשנות את השדה תאריך חשבונית במידה והוא מבצע שליחה חוזרת של החשבונית (כל סוג של חשבונית).**  קבלת ההחלטה לגבי היעד של המסר: ראה נספח יא |
| מסכי הפעולה | 1. יש לעדכן במסך צפייה בחשבוניות את סטאטוס החשבונית על פי הלוגיקה שמופיעה באיפיון מסר סטאטוס חשבונית. |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | הספק |
| מקבל | משהב"ט |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר | 1. איפיון מבנה המסר: ראה נספח טז 2. איפיון אלגוריתם שליחה לספקים מתווכים מקבלי המסר – נספח יא |

#### 2.5.20 שליחת הודעת זיכוי לספק

|  |  |
| --- | --- |
|  | **שליחת הודעת זיכוי לספק** |
| תיאור הנדרש | לאחר ביצוע תשלום בפועל לספק מוציא משהב"ט מסר הודעת זיכוי המכיל את פרטי התשלום שבוצע לספק ובגין איזו חשבונית. על המגיש להעביר לספק את הנתונים.  יש להיערך לריבוי מסרים פר חשבונית לצורך הצגת רצף סטאטוסים.  קבלת ההחלטה לגבי היעד של המסר: ראה נספח יא |
| מסכי הפעולה | 1. מסך צפייה לכל ספק בהודעות הזיכוי שלו. |
| תדירות | מאות - אלפים ביום |
| שעות פעילות ממשק | כל היום |
| שולח | משהב"ט |
| מקבל | הספק |
| טיפול בשגיאות סיסטם |  |
| פורמט תיאור מבנה מסר | XSD |
| איפיון וסרגל מבנה המסר | 1. איפיון מבנה המסר: ראה נספח יז 2. איפיון אלגוריתם שליחה לספקים מתווכים מקבלי המסר – נספח יא |

### 2.6 טבלאות קודים

#### 2.6.0 רשימת טבלאות

| # | שם הטבלה | תיאור הטבלה | סימול | סיווג |
| --- | --- | --- | --- | --- |
| 2.6.1 | טבלת סטטוסי חשבוניות | טבלת הקודים והמשמעויות של סטטוסי החשבוניות |  | מנהל פרויקט באישור משהב"ט בלבד |
|  |  |  |  |  |

#### 2.6.1 טבלת סטאטוס חשבוניות

| ערך מספרי לקוד | ערך תיאורי | משמעות |
| --- | --- | --- |
| 05 | חש.מרקט -קליטה ראשונית |  |
| 10 | קליטה ראשונית-חש. שגויה |  |
| 11 | קליטה ראשונית-חש. דיגיטלית |  |
| 40 | מסר חש. אושר לתשלום |  |
| 52 | מסר חשבונית שגוי/בבדיקה |  |
| 51 | מסר תמ"ש נקלט |  |
| 52 | מסר תמ"ש שגוי |  |
| 20 | חשבונית הוחזרה לספק |  |
| 63 | חשבונית בטיפול |  |
| 65 | חשבונית בטיפול |  |
| 41 | בוצע סטורנו לחשבונית |  |
| 16 | חשבונית שולמה |  |

### 2.7 דו"חות (ושאילתות) – לפורטל.

#### 2.7.0 אינדקס ורשימה כללית

הנ"ל רשימת דו"חות מינימליות.

| # | תיאור הדו"ח |
| --- | --- |
| 2.7.1 | דו"ח תנועות אחרונות |
| 2.7.2 | דו"ח לסוג תנועה ספציפית |
| 2.7.3 | דו"ח חיפוש לפי ערכים עסקיים |
| 2.7.4 | דו"ח קישור בין אובייקטים |

#### 2.7.1 דוח תנועות אחרונות

הגורם הדורש: ספקי המשרד

תאור כללי: מאפשר לראות מיידית תנועות אחרונות מול משהב"ט.

תדירות הפקת הדו"ח: על פי צרכי ספקי המשרד.

שיטת שפעול הדו"ח: אונליין.

הרשאה: כל ספק מוכר של המשרד אשר בא בהתקשרות עסקית עם המגיש יוכל להפעיל את הדו"ח תוך שמירת מידור חמור בין ספק לספק, כך שלא יצפה ספק אחד בנתונים של משנהו.

אופן הפקה: שאילתא למסך או קובץ להדפסה.

שדות להצגה(לכל הפחות): סוג הממשק, תאריך כניסה למערכות המגיש, שעת כניסה למערכות המגיש, תאריך יציאה ממערכות המגיש, שעת יציאה ממערכות המגיש, סטאטוס תנועה.

סינון: לאפשר על בסיס כל אחד מהשדות המוצגים, למעט שעות.

מיון: לאפשר על בסיס כל אחד מהשדות המוצגים.

Drill down: אפשרות לבצע על תנועה אחת מהרשימה.

#### 2.7.2 דוח לסוג ממשק ספציפי

הגורם הדורש: ספקי המשרד

תאור כללי: מאפשר לראות תנועות אחרונות מול משהב"ט, בחיתוך של סוג ממשק ספציפית.

תדירות הפקת הדו"ח: על פי צרכי ספקי המשרד.

שיטת שפעול הדו"ח: אונליין.

הרשאה: כל ספק מוכר של המשרד אשר בא בהתקשרות עסקית עם המגיש יוכל להפעיל את הדו"ח תוך שמירת מידור חמור בין ספק לספק, כך שלא יצפה ספק אחד בנתונים של משנהו.

אופן הפקה: שאילתא למסך או קובץ להדפסה על בסיס 10 ימים אחרונים.

שדות להצגה(לכל הפחות): סוג הממשק, תאריך כניסה למערכות המגיש, שעת כניסה למערכות המגיש, תאריך יציאה ממערכות המגיש, שעת יציאה ממערכות המגיש, סטאטוס תנועה.

סינון: לאפשר על בסיס כל אחד מהשדות המוצגים, למעט שעות.

מיון: לאפשר על בסיס כל אחד מהשדות המוצגים.

Drill down: אפשרות לבצע על תנועה אחת מהרשימה.

#### 2.7.3 דוח חיפוש לפי ערכים ספציפיים

הגורם הדורש: ספקי המשרד

תאור כללי: מאפשר לראות תנועות אחרונות מול משהב"ט, בחיתוך של סוג ממשק ספציפי ושל ערכים עסקיים הקשורים לשדות של נתונים הנשמרים עבור אותה סוג ממשק.

תדירות הפקת הדו"ח: על פי צרכי ספקי המשרד.

שיטת שפעול הדו"ח: אונליין.

הרשאה: כל ספק מוכר של המשרד אשר בא בהתקשרות עסקית עם המגיש יוכל להפעיל את הדו"ח תוך שמירת מידור חמור בין ספק לספק, כך שלא יצפה ספק אחד בנתונים של משנהו.

אופן הפקה: שאילתא למסך או קובץ להדפסה.

שדות להצגה(לכל הפחות): סוג הממשק, תאריך כניסה למערכות המגיש, שעת כניסה למערכות המגיש, תאריך יציאה ממערכות המגיש, שעת יציאה ממערכות המגיש, סטאטוס תנועה.

סינון: לאפשר על בסיס כל אחד מהשדות המוצגים, למעט שעות.

מיון: לאפשר על בסיס כל אחד מהשדות המוצגים.

Drill down: אפשרות לבצע על תנועה אחת מהרשימה.

#### 2.7.4 דוח קישור בין אובייקטים

הגורם הדורש: ספקי המשרד

תאור כללי: מאפשר לראות את היררכיית התנועות האחרונות מול משהב"ט, בחיתוך של סוג ממשק ספציפי ושל ערכים עסקיים הקשורים לשדות של נתונים הנשמרים עבור אותו סוג ממשק. יוצג בדוח החל מרמת הזמנה ועד רמת הודעת זיכוי. (ראה תיאור אובייקטים בנספח יב)

תדירות הפקת הדו"ח: על פי צרכי ספקי המשרד.

שיטת שפעול הדו"ח: אונליין.

הרשאה: כל ספק מוכר של המשרד אשר בא בהתקשרות עסקית עם המגיש יוכל להפעיל את הדו"ח תוך שמירת מידור בין ספק לספק, כך שלא יצפה ספק אחד בנתונים של משנהו.

אופן הפקה: שאילתא למסך או קובץ להדפסה.

שדות להצגה(לכל הפחות): סוג הממשק(תנועה), תאריך כניסה למערכות המגיש, שעת כניסה למערכות המגיש, תאריך יציאה ממערכות המגיש, שעת יציאה ממערכות המגיש, סטאטוס תנועה.

סינון: לאפשר על בסיס כל אחד מהשדות המוצגים, למעט שעות.

מיון: לאפשר על בסיס כל אחד מהשדות המוצגים.

Drill down: אפשרות לבצע על תנועה אחת מהרשימה.

## 3. טכנולוגיה ותשתית

### 3.1 תוכנת סוכן

לצורך בדיקת עמידת המגיש בתנאים האמורים מסכים המגיש לביקור המשרד או מי מטעמו כאמור בסעיף 1.3.0. זאת עבור כל אחד מסעיפי המשנה של סעיף זה.

על המגיש לחתום על הצהרה כמובא בנספח טו.

#### 3.1.0 ארכיטקטורה כללית

על מנת לבצע בפועל את תהליך העברת המסרים בין המגיש לבין המשרד יש צורך בחיבור טכנולוגי. בתהליך חיבור זה מתקני המשרד יהוו תמיד מוקד ייזום התקשורת, העברת המסרים לתוך משהב"ט תבוצע תמיד בייזום על ידי מערכות היושבות במתקני המשרד.

אמצעי החיבור יהיה תוכנת סוכן של המגיש אשר תשב על שרתים בחוות השרתים של המשרד ותיצור את ההתקשרות לשרתי המגיש.

על תוכנת הסוכן לעבוד במהירות, באמינות ובשקיפות. יש לאפשר פיתוח לצוות מיסור של המשרד בצורה פשוטה וקלה, וכן לאפשר גמישות בהגדרות. עליה לעמוד גם בנפחים ועומסים.

מטרת תוכנת הסוכן הינה לאפשר יכולת הורדת והעלאת קבצים אל שרתי המגיש. בתהליך ההעלאה נדרשת יכולת לאסוף קבצים מתיקיות שונות ברשת תוך יכולת הבחנה בין סוגי קבצים על בסיס סכימת שם קובץ(ראה סעיף 3.1.3). על התוכנה לאפשר איסוף ממספר מקורות במקביל עבור הגדרה אחת של סוג קובץ. על התוכנה לאפשר אירכוב של הקבצים הנאספים לתיקיות בשרתי המשרד.

בתהליך ההורדה של הקבצים נדרשות אותן יכולות של איסוף ממספר מקורות עבור הגדרה אחת של סוג קובץ והורדת הקבצים לתיקייה ברשת. נדרשת יכול אירכוב הקבצים המורדים לתיקייה נוספת ברשת.

#### 3.1.1 אחסנת נתונים מרכזית

תוכנת הסוכן חייבת להיות בעלת יכולת התקנה stand alone או בעלת מימוש מאגר נתונים פנימי,

כך שמשהב"ט לא יזדקק להעמיד את שירותי ה-DBA שלו.

#### 3.1.2 מערכת הפעלה

היה והמגיש יידרש להתקין תוכנת סוכן, עליה להיות מתאימה למערכת הפעלה windows של מיקרוסופט, וכן עליה להיות מותאמת לשרתים וירטואליים.

#### 3.1.3 כלי פיתוח ותחזוקה

נדרש שתהיה יכולת בסיסית למנהלן מטעם המשרד שאינו מומחה בתוכנה לבצע פעולות שינוי הגדרות של ניתובי מסרים ותחזוקה בצורה קלה ונהירה ללא צורך בקריאות שירות לספק המגיש.

על התוכנה לאפשר פיתוח בצורה פשוטה וקלה, כלומר או מסכי קונפיגורציה קלים או פיתוח באמצעות קבצים באופן שניתן ללומדו בחצי יום עד יום הדרכה. מבחן התוצאה הינו שתכניתן שעבר הדרכה כזאת בסוף היום מצליח להגדיר ממשק באופן עצמאי לחלוטין.

על תוכנת הסוכן לאפשר למנהלן לקבוע איסוף של קבצים מתיקיות ספציפיות והעברתם למגיש תוך שימוש בטכנולוגיה הרלוונטית למגיש. על התוכנה לאפשר להבחין בין סוגי מסרים שונים על בסיס שם תיקייה ו\או סכימת שם קובץ (מחוייב אבחנה בין סוגי מסרים על בסיס סכימת שם ייחודית גם אם שניהם באותה תיקייה).

סכימת שם הקובץ צריכה לאפשר שימוש בתווי ג'וקר בכל תצורה אפשרית, לדוגמא: \*val\*, \*val1\*val2\* וכו'.

באיסוף קובץ התוכנה חייבת לאפשר מחיקה או השארת הקובץ תוך סימונו כ-read only או העברתו לתיקיית ארכיון.

התוכנה תדרוש מינימום תחזוקה חיצונית, עד יום אחד של טכנאי בשנה.

התוכנה תאפשר שידרוגים ע"י התקנה פשוטה של קובץ שיועבר למשהב"ט ללא צורך בשליחת טכנאי.

#### 3.1.4 כלי תפעול וייצור

יש לאפשר אתחול של התוכנה במקרה של תקיעה.

יש לאפשר גמישות ושליטה בזמני ההפעלה של התוכנה: service שנמצא באוויר כל הזמן וניתן להפסקה או scheduled task שניתן לשליטה.

#### 3.1.5 כלי שליטה ובקרה למנהל המערכת

יש לאפשר גישה למנהלן המערכת למערכת הדיווח של תוכנת הסוכן על מנת לאתר מסרים. מערכת הדיווח חייבת לאפשר חיתוך מינימאלי של הלוגים על בסיס סוג מסר.

על התוכנה לדווח על כל שאל מפעילותה לרבות שגויים, ולאפשר שקיפות למנהלי המערכת בפתרון תקלות.

כל תנועה בתוכנה צריכה להיות מדווחת על בסיס המינימום של פרמטרים הבאים: שם תיקייה, שם קובץ, תאריך ושעה. הפרמטרים המינימליים האילו ידווחו עבור כל פעולה של איסוף, יצירת או אירכוב קובץ.

#### 3.1.6 עומסים וביצועים

על התוכנה לסיים טרנזאקצייה של העברת מסר בהצלחה תוך 0.5 שניות, במצב שבו ממתינים לשליחה אלפי מסרים בו זמנית.

על התוכנה להיות בעלת יכולת לטפל בקבצים גדולים של עד כ-2GB.

על התוכנה לנהל את הטרנזקציות באופן כזה שלא יאבד אף מסר, והשגויים ידווחו ויישמרו במאגר לשליחה חוזרת.

#### 3.1.7 אבטחת מידע

מתוכנת הסוכן נדרשת יכולת הפעלת אמצעי החיבור לשרתי המגיש בצורה מוצפנת.

נתוני ההגדרות שיבוצעו בתוכנה יישארו בצד המשרד ולא יועברו מחוץ לשרת עליו יושב.

### 3.2 אבטחת מידע

#### 3.2.0 כללי

בסעיף זה מתוארות הדרישות ליישום אבטחת מידע עפ"י דרישות הרגולציה, לפעולות המערכת.

מוצרים או פתרונות אבטחה אשר אינם מוכרים בעולם ו\או בארץ ואשר מוצעים על ידי המציע ליישום במסגרת בקשה לסיווג ספקים זו, חובת ההוכחה על יעילות האבטחה באמצעות פתרונות אלה יהיה על המציע. יהיה עליו לספק דוגמאות למקומות נוספים בארץ ובעולם בהם הפיתרון מיושם בהצלחה

#### 3.2.1 סיכוני אבטחת מידע (במ"ם)

**שמירת סודיות - Confidentiality**

מידור: חשיפת מידע של משרד הבטחון בפני לקוחות אחרים של המגיש;

חשיפת מידע של ספק אחד למשנהו.

זליגת מידע: חשיפה של המידע לגורם חיצוני שלא קשור לשרשרת האספקה, חשיפת המידע לגורם עוין.

**אמינות המידע - Integrity**

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

**זמינות המידע- Availability**

מניעת שירות- DOS: הפלת מערכתה המידע של המגיש וגרימת הפסקת שירות כתוצאה מכך.

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

#### 3.2.2 אמצעי אבטחת מידע (במ"ם)

1. מערכות המגיש תהיינה מאובטחות באמצעות טכנולוגיות ואמצעי אבטחת מידע המקובלים בשוק על מנת להבטיח רמת אבטחת מידע גבוהה, הנדרשת למערכות מסחר רב-צדדיות, וכמקובל במגזר העסקי לאבטחת מערכות מסחר אלו.

2. המגיש יגדיר מדיניות ויממש מידור קפדני, שתמנע חשיפה של נתוני לקוח אחד ללקוח שני, ונתוני ספק אחד לספק אחר.

3. המגיש ישלב במערכת אמצעים המקובלים בשוק למניעת התקפות על מערכות המגיש, כמפורט בסעיפים 3.2.3, 3.2.4, 3.2.5.

4. המגיש יציין את שמו של המנהל או האחראי על אבטחת מידע בארגון, הכשרתו והסמכותיו, ויפרט את פרטי הקשר שלו.

5. המגיש יצרף עותק של מדיניות אבטחת המידע הארגונית, ואת נהלי האבטחה המיושמים בכדי לעמוד באמור במסמך המדיניות.

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

7. הבקרה השוטפת על רמת אבטחת המידע תבוצע לפי המפורט בנספח אבטחת המידע להגנת הפרטיות, המצורף למסמך זה כנספח ה, אותו יש למלא ולהגיש כחלק מהמענה לסעיף 3.2.

#### 3.2.3 אבטחת תשתיות תקשורת

1. המגיש יתקין את מערכות המסור המוצעות בסגמנט רשת מופרד מכל מערכת אחרת של המגיש שאינם חלק ממערכת המסור.
2. הסגמנטציה המוצעת תכלול הפרדה מיטבית מאיומי רשת האינטרנט, ותבטיח צמצום האיומים למול משרד הבטחון וספקיו.
3. המגיש יתקין, יתפעל ויעדכן מערכות אבטחת תשתיות ותקשורת מקובלות בענף, אשר יכללו לכל הפחות :
   1. חומת אש– FireWall
   2. מערכת למניעת חדירות - IPS
   3. אנטי וירוס ומניעת תוכנה זדונית - Anti-Virus
4. כל רכיבי האבטחה יהיו ייעודיים למערכת המסרור, ולא יהיו משותפים בדרך כלשהי עם גורמים או מערכות אחרות שאינם חלק ממערכת המסרור.
5. המגיש יגדיר חוקים אשר ימנעו חדירה למערכת, ויבקר באופן שוטף את יעילות החוקים באבטחת המערכת.
6. המגיש יתאים את אמצעי אבטחת המידע לאיומים, כפי שיוגדרו ע"י המגיש במשותף עם משרד הבטחון מעת לעת.
7. המגיש ירשום כל פעילות במערכות התקשורת ורכיבי אבטחת המידע באמצעות יומן פעולות (Audit Log) ויבקר אותו כמוגדר בסעיף המתאים במסמך זה.
8. אבטחת המידע כאמור – תיושם באופן מלא גם באתר ה-DR באם מוצע.
9. למען הסר ספק – ידוע וברור כי מערכת המסרור המוצעת תשמש במקביל לקוחות רבים של המגיש, והדרישה להפרדה הינה של של מערכת המיסור עצמה ממערכות או טכנולוגיות אחרות שהמגיש עשוי להפעיל במסגרת פעילותו העסקית.

#### 3.2.4 אבטחת שרתים והקשחות

1. שרתי המערכת יאובטחו ויוקשחו באופן שוטף, בפרק זמן סביר מפרסום הטלאים  ולפי כללי ה- Best practice המקובלים בענף.
2. המגיש 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.
3. עמדות הקצה לניהול המערכת יאובטחו בפני תוכנה זדונית, ובפני הכנסה והוצאת מדיה נתיקה.
4. המגיש יתאים את אמצעי אבטחת המידע לאיומים, כפי שיוגדרו ע"י המגיש במשותף עם משרד הבטחון מעת לעת.
5. המגיש יתעד כל פעילות בשרתי המערכת באמצעות יומן פעולות (Audit Log) ויבקר אותו כמוגדר בסעיף המתאים במסמך זה.
6. אבטחת המידע כאמור – תיושם באופן מלא גם באתר ה- DRבאם מוצע.
7. המציע יאחסן את מדיית הגיבוי באופן מאובטח, ויצפין את הנתונים האגורים במדיית הגיבוי או כל מדיה שליפה אחרת, באמצעות סיסמה שלא תהא ידועה או נגישה למבצעי הגיבויים.

#### 3.2.5 אבטחת אפליקציות

1. האפליקציות הפועלות במערכת יאובטחו לפי best practices מוכרים בשוק, כגון לפי כללי OWASP.
2. כל האפליקציות יוקשחו למניעת החדרת קוד זדוני, וביצוע פעולות כגון SQL injection, XSS וכו', לרבות עבור שרתי המערכת, עמדות הניהול אצל המגיש, תוכנת הניהול שתותקן במשרד הבטחון, ותוכנות הקצה אשר יותקנו אצל הספקים.
3. אבטחת האפליקציות תתבצע באמצעות יישום אבטחה בקוד, ו/או באמצעות שימוש ב- Application Firewall(WAF), או שילוב של הפתרונות.
4. פתרונות האבטחה יותאמו לטכנולוגיית היישום, בין אם כמערכת בתצורת שרת לקוח (EXE) או בתצורת דפדפן (Browser).
5. המגיש יתאים את אמצעי אבטחת המידע לאיומים, כפי שיוגדרו ע"י המגיש במשותף עם  משרד הבטחון מעת לעת.
6. המגיש יתאר את מנגנון מידור המידע הלוגי הקיים במערכת, המבטיח מידור מידע מלא בין ספקים שונים, ובין לקוחות שונים של המגיש לבין המידע המועבר לטובת משרד הבטחון.
7. המגיש ירשום כל פעילות אפליקטיבית חריגה במערכת באמצעות יומן פעולות (Audit Log) ויבקר אותו כמוגדר בסעיף המתאים במסמך זה.

#### 3.2.6 הצפנת מסרים ואימות זיהוי

1. כל תעבורת התקשורת, בין המגיש למשרד הבטחון, ובין המגיש לספקים, תוצפן באמצעות אמצעי הצפנה סטנדרטיים.
   1. המגיש יפרט מהי טכנולוגיית ההצפנה המוצעת וכיצד תיושם, בין אם באמצעות רכיבי VPN, או באמצעות הצפנות המקובלות בדפדפנים – ברמת ssl v3.
   2. המגיש יפרט כיצד ממומש מנגנון ההצפנה בתקשורת, ובאם ממומש ssl-v3 יפרט גם כיצד נמנע fall back ל-ssl-v2.
2. אימות זיהוי – שלב א' (חובה ליישום)
3. מנגנון אימות זהות הצדדים בתקשורת באמצעות ממשק webgui יהיה באמצעות שם משתמש וסיסמא ולפי בחירת הספק גם באמצעות זיהוי חזק בלבד, כאמור בסעיף הבא.
4. המציע יוודא ויצהיר 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.
5. המציע יתאר את מנגנון אימות הזיהוי הממומש אצלו, והאם ממומש באמצעות מנגנון בפיתוח עצמי או מנגנון המבוסס על רכיבי מערכת ההפעלה.
6. 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.
7. 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.
8. אימות זיהוי – שלב ב' (עתידי – לא ליישום כרגע)
9. הספק יצהיר כי ידוע וברור לו, כי במועד מאוחר יותר, אם תוך מספר חודשים או אף מספר שנים לאחר התחלת תפעול המערכת, תועלה דרישה כי לצורך העברת חלק מהמסרים או כולם יידרש הספק לממש פתרון של הזדהות חזקה, וזאת לאור נסיבות משתנות מסוגים שונים, כגון עדכון דרישות חוק, רגולציה, או מסיבות עסקיות באשר הן.
10. עם התממשות דרישה כזו לביצוע הזדהות חזקה, יממש המציע מנגנון הזדהות חזקה כאמור בסעיפים להלן, ואחרת, ללא מימוש מנגנון הזדהות חזקה כנ"ל, לא יוכל לספק שרותי מסרור לסוגי המסרים אשר העברתם תחייב באותה עת מימוש הזדהות זו, והספקים אשר פועלים להעברת מסריהם דרך המציע, יופנו להעברת המסרים באמצעות מפעילי מסרור אשר יציעו במועד הנדרש את אימות הזיהוי הנדרש.
11. למען הסר ספק – עם הגשת הצעה זו אין צורך לפרט מהו פתרון אימות הזיהוי החזק שימומש בעתיד, ויש רק להצהיר כי דרישות סעיף זה למימוש עתידי של הזדהות חזקה ומשמעויותיו ברורות למציע.
12. מנגנון אימות זהות הצדדים בתקשורת באמצעות ממשק webgui יהיה באמצעות זיהוי חזק בלבד – 2 factor authentication באמצעות טכנולוגיית סיסמא חד-פעמית OTP – One Time Password בלבד.
13. מנגנון אימות זהות הצדדים בתקשורת VPN ישירות למערכות הספק יהיה באמצעות זיהוי חזק בלבד – 2 factor authentication באמצעות תעודות דיגיטאליות שיונפקו על ידי גורם מורשה לפי חוק חתימה אלקטרונית 2001.
14. המגיש יפרט מה המוצר הטכנולוגי באמצעותו מוצע לממש את הזיהוי החזק, (התקן פיזי, תוכנה בסלולר וכו') וכיצד ימומש ניהול מערך הסיסמא החד-פעמית.
15. אם יש למציע משתמשים חיצוניים לצרכי תחזוקה או בקרה וכו', יש להציג את מתכונת האבטחה, שתכלול הזדהות ע"י OTP, או כרטיס חכם, ותווך של SSL VPN.
16. חתימה אלקטרונית והצפנת תוכן המסרים (עתידי – לא ליישום כרגע)
17. הספק יצהיר כי ידוע וברור לו, כי במועד מאוחר יותר, אם תוך מספר חודשים או אף מספר שנים לאחר התחלת תפעול המערכת, תועלה דרישה כי לצורך העברת חלק מהמסרים או כולם יידרש הספק לממש פתרון של חתימה אלקטרונית למסרים, וזאת לאור נסיבות משתנות מסוגים שונים, כגון עדכון דרישות חוק, רגולציה, או מסיבות עסקיות באשר הן.
18. עם התממשות דרישה כזו לביצוע חתימה אלקטרונית והצפנת תוכן המסרים, יממש המציע מנגנון כנדרש במפורט להלן, ואחרת, ללא מימוש מנגנון חתימה והצפנה כנ"ל, לא יוכל לספק שרותי מסרור לסוגי המסרים אשר העברתם תחייב באותה עת מימוש כזה, והספקים אשר פועלים להבערת מסריהם דרך המציע, יופנו להעברת המסרים באמצעות מפעילי מסרור אשר יציעו במועד הנדרש את המנגנון הנדרש.
19. למען הסר ספק – עם הגשת הצעה זו אין צורך לפרט מהו פתרון החתימה האלקטרונית והצפנת תוכן המסרים שימומש בעתיד, ויש רק להצהיר כי דרישות סעיף זה למימוש עתידי ומשמעויותיו ברורות למציע.
20. המגיש יציע פתרון למימוש חתימה אלקטרונית לתוכן המסרים, באמצעות תעודה דיגיטלית העונה על דרישות חוק חתימה אלקטרונית 2001, ויצפין את תוכן המסרים והקבצים המצורפים להם, אשר עבורם התבקש במפורט, באמצעות אלגוריתם הצפנה סטנדרטי המקובל בשוק.
21. המגיש יפרט מהו אלגוריתם ההצפנה אשר מוצע, והאם זהו אלגוריתם סינכרוני כגון DES, 3DES או AES, או אלגוריתם א-סימטרי מבוסס PKI.
22. המגיש יפרט את מנגנון וידוא אמינות ומקוריות המסרים המועברים ודרך הצגתם לספקים ולנציגי משרד הבטחון, תוך הבטחת שימושיות מירבית להבטחת אמינות ומקוריות תוכן המסרים. .

#### 3.2.7 מניעת זליגת מידע

1. המגיש יתקין ויתפעל אמצעים למניעת זליגת מידע מהמערכת, לגורמים שאינם מורשים על ידי משרד הביטחון. האמצעים המוצעים יפורטו ע"י המציע, כדלהלן:
   1. מוצר DLP
   2. הקשחת עמדות קצה
   3. מניעת גישה למדיה ו-USB בעמדות קצה
2. המגיש 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:
   1. הגדרת גישה למידע לפי הצורך לדעת – Need To Know
   2. הצפנת מספרי כרטיסי אשראי
   3. הסתרת ספרות כרטיסי אשראי כנדרש (תצוגת 4 ספרות אחרונות בלבד)
   4. הצפנה ומידור מידע רפואי.
3. המגיש יתאר באופן מדוייק 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.

#### 3.2.8 עובדי המגיש

1. כל עובד של המגיש ישתמש בחשבון משתמש וסיסמא אישיים בלבד בגישה לכל מערכת או בסיס נתונים, ולא ייעשה שימוש כלשהו בחשבונות משתמש משותפים, לרבות עבור חשבונות ניהול פריבילגיים.
2. המציע יפרט מהו תהליך בדיקת המהימנות המבוצע ע"י המגיש עבור העובדים אשר יועסקו בפיתוח ותחזוקה של המערכת, טרום העסקתם בתפעולה.
3. משרד הביטחון שומר לעצמו את הזכות לדרוש מהמגיש להעביר באופן תקופתי את פרטי העובדים הרלבנטיים וכל שינוי בהם, ואת תוצאות בדיקת המהימנות שעברו. תפעול המערכת ופיתוחה יבוצע רק ע"י עובדי המגיש אשר  עברו את כל בדיקות המהימנות והמיומנות מטעם המגיש, וחתמו מראש על טופס שמירת הסודיות. העתקים מטופסי שמירת הסודיות ביחד עם תוצאות בדיקות המהימנות, יועברו למשרד הבטחון , מבלי להטיל אחריות כלשהי על משרד הבטחון.
4. משרד הבטחון שומר לעצמו את הזכות להטיל וטו על העסקת עובד מסוים של המפעיל, ללא מתן הסבר, מבלי שהדבר יגרע מאחריות המפעיל או יטיל אחריות כלשהי על משרד הבטחון.

#### 3.2.9 אבטחה פיזית

1. נדרש מתקן סגור, מאובטח 24/7, עם חדר מחשבים נעול ומאובטח באמצעות אזעקה וטלויזיה במעגל סגור. הארון שיכיל את השרתים יינעל ויאובטח באמצעות אזעקה. כל פתיחה שלו שלא בשעות העבודה הרגילות - תשלח מסר למשרד. נדרש דיווח למשרד על כל אירוע אבטחתי במתקן.
2. יש להשתמש בכלי ניטור להתראה בפני גישה לא מורשית לשרתים.

#### 3.2.10 בקרות אבטחת מידע

1. המגיש יבצע בקרות אבטחת מידע שוטפות על המערכת, על כלל רכיביה, על מנת לוודא עמידתו בדרישות אבטחת המידע
   1. הבקרות השוטפות יכללו בין היתר ניתוח ממוכן של נתיב הביקורת כאמור בסעיף 3.2.5 ו-3.2.6, 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 משרד הבטחון מעת לעת להבטחת עמידת המגיש בהתחייבותיו.
   2. המגיש יתחייב לבצע בקרות ובדיקות אבטחת מידע לפי דרישת משרד הבטחון, בין אם לאור אירועים שונים, חשדות לאירועים, או בשל סיבה או צורך אחרים כלשהם.
   3. המגיש יתאר בהצעתו את היקף הבקרות המוצע, תדירותם, ואת הגורם המוצע לבצע את הבקרות הנדרשות, ואשר יעמוד בדרישות המפורטות בתת סעיף ב' להלן.
   4. המגיש יתחייב לבצע סקר אבטחת מידע מקיף על המערכת בתדירות אשר תבטיח את בחינת כלל המערכות לפי רמת רגישותן במחזוריות של לפחות אחת ל-18 חודשים.
   5. תיקון הליקויים אשר יימצאו בבקרות אבטחת המידע הללו יתוקנו לפי הלו"ז המוגדר בסעיף 3.2.11 ב' להלן.
2. המגיש 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 המגיש, ומצא אותה עונה על עיקרי הדרישות המובעות במסמך זה.
3. המגיש יציג תוכנית תגובה לאירועי אבטחת מידע שמזוהים, כולל כל ניסיון חדירה או דליפה של המידע המוחזק של המשרד, וכל ניסיון חדירה או דליפה אחר למערכות הספק, שאיננו קשור ישירות למידע של המשרד.

#### 3.2.11 ביקורות אבטחת מידע

1. משרד הבטחון (באמצעות יועצים מומחים), יבצע מעת לעת ביקורות אבטחת מידע בהתאם לצרכיו, ולפי דרישות חוק הגנת הפרטיות ותקנות רישום מאגרי המידע.
2. המגיש יפעל לתקן כל ליקוי אשר יימצא בביקורות אלו בתוך פרק זמן סביר כמקובל בענף, בנסיבות העניין.
   * 1. תיקון  ליקויים קריטיים – יחל באופן מיידי ויושלם תוך 4 שבועות לכל היותר.
     2. תיקונים  מהותיים שאינם חשיפות קריטיות -  יבוצעו תוך 20 ימי עסקים ויושלמו בהקדם האפשרי.
     3. תיקון ליקויים שאינם מהותיים ואינם קריטיים -  יתוקנו תוך 60 ימי עסקים לכל היותר.
3. תיקונים אשר יתברר על ידי המגיש כי תיקונם ייארך משך זמן ארוך יותר בשל נסיבות אוביקטיביות, יועלו לדיון במשותף עם  משרד הבטחון, ותתקבל החלטה משותפת לגבי לו"ז התיקון.

#### הבטחת רציפות השירות והיערכות לשעת חירום

#### מערך ה-DR נדרש על מנת לעמוד ב-SLA שנקבע בסעיף 4.3

1. המציע יפרט מהם האמצעים והפתרונות המוצעים על ידו להבטחת רציפות השירות. יש לפרט מהם האמצעים הקיימים כיום, ואילו אמצעים ייושמו לטובת הצעה זו:
   1. יתירות שרתים ורכיבי תקשורת – Redundancy
   2. Load Balancing
   3. כפילות קווי תקשורת
   4. אמצעים נוספים
2. המציע יפרט באם ברשותו מערך היערכות לשעת אסון (DR) הנועד להבטיח שירות באם תושבת פעילות אתר המחשבים הקבוע של המציע. יש לפרט את יכולות מתקן החירום והנהלים הקיימים כיום, ואילו אמצעים מוצע ליישם לטובת הצעה זו:
   1. מקום מתקן החירום והמרחק מהאתר הראשי.
   2. אמצעי המחשוב הקיימים באתר החירום, תשתיות תקשורת ורכיבי אבטחת מידע.
   3. פירוט יכולת מתקן החירום לספק רמת שירות סבירה או בהיקף אחר מוצע כלשהו.
   4. נהלי המעבר לאתר החירום ונהלי תפעולו - DRP.

#### נתיב ביקורת

בסעיף זה יתוארו הדרישות לנתיב ביקורת נדרש לפעולות המערכת.

### 3.2.13.0 נתיב ביקורת תשתיתי

1. המערכת תייצר נתיב ביקורת -Audit Log (יומן פעולות) עבור כל רכיבי התשתית הכלולים במערכת: שרתים, בסיסי נתונים, רכיבי תקשורת ורכיבי אבטחת מידע, אשר ירשמו ביומן פעולות מתאים.
2. . רישום הפעולות יכלול לפחות את הפעולות כגון:
3. כל בקשת הזדהות מוצלחת/כושלת
4. כל הוספה/עדכון מידע/פרמטרים במערכת
5. פעולות תקשורת מהותיות (כגון חיבור אתרים, ניתוקם, שינוי תעבורת תקשורת וכו')
6. כל שאילתא לאיחזור מידע כלשהו של משהב"ט במערכת
7. כל פעילות ניהול (אדמיניסטרציה) של המערכת
8. כל פעולת עדכון ו/או שינוי בתוכנה אפליקטיבית ו/או תשתיתית
9. אחסון נתיב הביקורת:
10. המערכת תאחסן את נתיבי הביקורת ביומן הפעולות בבסיס נתונים נפרד ומאובטח, למשך תקופה של שלושה חודשים אונליין ועד 24 חודשים באיחסון אופליין, מקליטת הנתונים.
11. נתוני נתיב הביקורת לא יהיו נגישים למחיקה או שינוי כלשהו, גם בפני אנשי הסיסטם והתוכנה של מגיש השירות.
12. המגיש יפרט את המתכונת המוצעת לאחסון מאובטח של נתיב הביקורת.
13. ניתוח יומן הפעולות:
14. ניתוח יומן הפעולות ותחקורו ישמשו לאיתור ניסיונות חדירה למערכת ואיתור פעולות חריגות ע"י גורמים פנימיים וחיצוניים, הן בזמן אמת והן בדיעבד.
15. ניתוח יומן הפעולות יבוצע באמצעות כלי ממוכן.
16. המגיש יפרט איזה פתרון מוצע לניתוח יומן הפעולות, ויתאר את הצעתו ליישום הפתרון ותפעולו השוטף לאיתור פעולות חריגות וניסיונות פריצה למערכת.

### 3.2.13.1 נתיב ביקורת אפליקטיבי

1. המערכת תייצר יומן פעולות עבור כל כל רכיבי התוכנה המופעלים במערכת לרבות: תוכנת אפליקצית המיסור, התוכנה המותקנת במשרד הבטחון, התוכנות המותקנות אצל הספקים. רישום הפעולות יכלול פעולות כגון:
2. כל מסר של ספק למשהב"ט
3. כל מסר של משהב"ט לספק
4. כל הוספה/עדכון מידע והרשאות במערכת
5. כל עדכון גירסת תוכנה ו/או רכיב תוכנה במערכת (יומן שינויים)
6. כל שאילתא לאיחזור מידע כלשהו במערכת
7. המערכת תאחסן את נתיבי הביקורת ביומן הפעולות בבסיס נתונים נפרד ומאובטח, למשך תקופה של שלושה חודשים באונליין ועד ל-24 חודשים באופליין.

1) נתוני נתיב הביקורת האפליקטיבי לא יהיו נגישים למחיקה או שינוי כלשהו,  
     גם בפני אנשי הסיסטם והתוכנה של המגיש.

2) המגיש יפרט את המתכונת המוצעת לאחסון מאובטח של נתיב הביקורת  
     האפליקטיבי.

1. ניתוח יומן הפעולות:
   * + 1. ניתוח יומן הפעולות ותחקורו ישמשו לאיתור ניסיונות חדירה למערכת ואיתור פעולות חריגות ע"י גורמים פנימיים וחיצוניים, הן בזמן אמת והן בדיעבד.
       2. ניתוח יומן הפעולות יבוצע באמצעות פתרון כלי ממוכן.
       3. המגיש יפרט איזה פתרון מוצע לניתוח יומן הפעולות, ויתאר את הצעתו ליישום הפתרון ותפעולו השוטף לאיתור פעולות חריגות וניסיונות פריצה למערכת.

#### שימוש בשירותי ענן צד ג'

שימוש בשירותי ענן ליישום מערכת "קשר דיגיטלי מסחרי" מותר, תוך עמידה מלאה בהתניות המפורטות להלן, למרות שתינתן עדיפות מלאה לתפעול המערכת בשרתים פרטיים של מפעיל השירות.

### 3.2.14.1 דרישות לבחירת ספק שירותי ענן לאתר הייצור של המערכת

1. אירוח המערכת בשירותי ענן באתר הייצור מותר כל עוד האירוח מתבצע בחוות שרתים הממוקמת פיזית בישראל, ומרכז התפעול ותמיכה שלה ממוקם אף הוא בישראל.
2. נדרש לבחור ספק שירותי "ענן ציבורי" מחברה מוכרת ומובילה בישראל.
3. השרתים יהיו שרתים ייעודיים עבר מפעיל מערכת "קשר דיגיטלי מסחרי", או לכל הפחות מערכת וירטואלית ייעודית המוגדרת עבור המערכת – VPC. (Virtual Private Cloud).
4. עומדת בדרישות אבטחת המידע הייעודיות לענן כמפורט להלן.

### 3.2.14.2 דרישות לבחירת ספק שירותי ענן לאתר הגיבוי(DR) של המערכת

1. אירוח המערכת בסביבת שירותי ענן למטרות DR, מותר בארץ או בחו"ל, בהתניות המפורטות להלן.
2. המערכת תתארח במתכונת של שרתים ייעודיים עבור המערכת או VPC.
3. אם המערכת איננה מתארחת במערך שרתים ייעודי או סביבה וירטואלית ייעודית, ו/או מתאחרת אצל ספק שירותי ענן בחו"ל/שירות בינ"ל, חובה להצפין את כל המידע האגור במערכת – הצפנת מידע נייח, כאשר לספק שירותי הענן לא יתאפשר בשום דרך לגשת אל המידע המאוחסן בשרתים כמידע גלוי, וסיסמת הפענוח תימצא אר ורק בידי מפעיל המערכת.

### 3.2.14.3 דרישות אבטחת מידע כלליות עבור יישום אירוח בסביבת "ענן ציבורי"

1. אבטחת תקשורת: כל התקשורת בין סביבת המיחשוב של המפעיל, לסביבת "הענן" תוצפן באמצעות פתרון הצפנה מסחרית מוכרת, עם יישום תעודות דיגיטליות בשני הצדדים, לפי תקן TLS 1.2, מאושר Fips 140-2.
2. חובה ליישם במתכונת אירוח הענן את כל אמצעי אבטחת המידע המפורטים במסמך הבקשה לשירות "ספק מורשה קשר דיגיטלי מסחרי", לרבות אנטי-וירוס/קוד זדוני, FW וכו'.
3. יישום IPS ו – WAF חייב להתבצע ע"י פתרון ייעודי עבור מפעיל השירות. היישום יכול להתבצע ע"י מערכך אבטחה פיזי או וידרטואלי, אך יובהר כי ניהולו והשליטה בהגדרותיו חייבת להיות בשליטה מלאה של מפעיל השירות.
4. יש לפרט את מתכונת המעבר המתכוננת לאתר החירום לכשיידרש מעבר כזה, מתי מתוכנן לעבור לאתר החירום ובאילו נסיבות, וכן את מתכונת החזרה לשגרה.
5. יש לצרף פירוט מלא ומפורט של מתכונת האירוח בשירותי ענן.
6. הפירוט יכלול את מתכונת האירוח, זהות מנהלי השרתים / מערכות הפעלה / תקשורת / תמיכה טכנית
7. אמצעי האבטחה המיושמים, לרבות אלו הנרכשים כשירות מספק הענן
8. אילו אמצעים מיושמים באופן עצמאי (שלא באמצעות ספק שירותי הענן).
9. הפירוט יכלול שמות מוצרים, גירסאות וכו'.
10. אם נעשה שימוש בהצפנת מידע נייח – יש לספק מידע מלא על מתכונת ההצפנה, המוצר בשימוש, כיצד מנוהלים מפתחות ההצפנה וכו'.

### 3.2.14.4 בקרה על ספק שירותי הענן

1. יש לספק מידע על מתכונת הבקרה על ססטוס האבטחה של המערכת המתארחת בענן, זיהוי אירועי אבטחה שהתרחשו, וכיצד מדווח המפעיל על אירועים כאלו.
2. בקרה על שינוי הגדרות המערכת ע"י ספק שירותי הענן, לרבות עבור:
3. שרתים/מערכות הפעלה/ניהול חשבונות וכו'
4. ציוד תקשורת
5. מערכות אבטחת מידע – כגון שינוי חוקי FW
6. בקרה על עדכון מערכות האבטחה והשרתים ע"י ספק שירותי הענן.

### 3.2.14.5 מידור המידע מספק שירותי הענן ועובדיו

1. יש לתאר כיצד אמצעי האבטחה שיושמו, ו/או הגדרות של אפליקציית המערכת, משמשים לטובת מידור ספק שירותי הענן ועובדיו, מגישה למידע של משרד הבטחון.
2. יש לבאר כיצד מסוגל המפעיל לבקר כי ספק שירותי הענן לא ניגש בפועל למידע המאוחסן במערכותיו, בין אם בגישה ישירה, או עקיפה (Virtual machine cloning) וכו'.

### 3.2.14.6 מעבר לספק שירותי ענן אחר

1. אם המפעיל מתכנן מעבר לספק שירותי ענן אחר, יש לספק למשרד הבטחון מראש ובכתב מידע על תוכנית זו, לפי המתכונת המפורטת בסעיפים המפורטים כאן.
2. התוכנית למעבר תכלול פירוט מלא על מתכונת ביעור המידע המתוכננת אצל הספק המוחלף.
3. אין לעבור בפועל לספק שירותי ענן אחר ללא אישור מראש ובכתב של משרד הבטחון.

### 3.3 דרישות פיתוחיות מערכת מרכזית

לצורך בדיקת עמידת המגיש בתנאים האמורים מסכים המגיש לביקור המשרד או מי מטעמו כאמור בסעיף 1.3.0. זאת עבור כל אחד מסעיפי המשנה של סעיף זה.

#### 3.3.1 דרישות ESB ממערכת המיסור המרכזית

בסעיף זה יתוארו הדרישות לנתיב ביקורת נדרש לפעולות המערכת.

### 3.3.1.1 ניתוב

1. יכולת ניתוב ליעדים שונים של מסר.
2. יכולת ניתוב על בסיס ערכים בשדות שונים במסר (ללא קשר לפורמט המסר: XML,FLAT).
3. יכולת פיצול מסר כללית.
4. יכולת פיצול מסר על בסיס ערכים בשדות שונים במסר.

### 3.3.1.2 מיפויים\טרנספורמציות

1. יכולת לבצע מיפויים וטרנספורמציות בפורמטים הבאים: XML ל-XML, XML ל-FLAT, FLAT ל-XML, FLAT ל-FLAT, EXCEL ל-XML, XML ל-EXCEL.
2. יכולת המרה מכל encoding שהוא לכלencoding שהוא.
3. יכולת סינון סגמנטים נתונים על פי לוגיקה המבוססת על ערכים במסר.
4. יכולת איסוף מספר קבצים לקובץ זיפ.
5. יכולת פתיחת קובץ זיפ לקבצים המכילים אותו.
6. באם נדרשה על ידי ספק כלשהוא טרנספורמציה ממסר המקור אל מסר היעד (ללא קשר לכיוון), על המגיש לתת מענה בתוך 20 יום מרגע ביצוע ההתקשרות העיסקית ביניהם הנוגעת לטרנספורמציה.

### 3.3.1.3 קישוריות

1. יכולת ביצוע ואלידציה על סכימות של XML חובה. יכולות נוספות של ואלידציה על קבצים שונים מ-XML כדוגמת שטוחים, CSV וכן הלאה אינו חובה אך ייחשב כיתרון.
2. יכולת עבודה מול כספות cyberark, הכוללת יכולת למשוך מהכספת ולהוריד לקבצים ויכולת לאסוף קבצים מתיקיות והעלאתן לכספת.
3. יכולת עבודה בקבצים מול FTP או SFTP.
4. יכולת הפעלה של web services כצרכן ויכולת להעמיד web services לצריכה של חיצוניים.
5. יכולת בניית שם קובץ למסר הכולל ערכים עיסקיים אשר נלקחים מתוך תוכן המסר.

### 3.3.1.4 תהליכים עיסקיים

1. יכולת תפירה של תהליך עיסקי בו המסר עובר תחנות בהן מתבצעות העשרות או מניפולציות על המסר ו\או עידכון או שליחה של נתונים אל מול מערכות חיצוניות.

### 3.4 נפחים עומסים וביצועים

1. מערכות המגיש מחויבות לעמוד בסטנדרטים מחמירים של עמידות ושרידות, עקב העובדה שאופיין של חלק ממערכות משהב"ט הינו מבצעי.
2. שירותי ה-B2B והפורטל בסביבת הייצור יהיו זמינים 24\*7.
3. סביבת בדיקות חיה ופועלת ללא צורך בהתערבות ידנית בזמינות מלאה בימי העבודה בשעות שבין 7 בבוקר ועד 20:00.
4. על מערכות המגיש להיות מסוגלות לעמוד בסדרי גודל של 100,000 מסרים בממוצע ביום הנשלחים אל ומתקבלים ממשהב"ט, עם עומסים עולים ויורדים במהלך היום.
5. על מערכות המגיש להיות בעלי יכולת לסיים טיפול במסר B2B (ללא שגיאות) עד 5 שניות מקצה לקצה.

## 4. שירות ו-SLA

### 4.0 כללי

בסעיף זה יידון נושאי שירות לקוחות ו-SLA של המגיש כלפי המשרד וכלפי הספקים.

### 4.1 צוותים נדרשים

#### 4.1.0 שירות לקוחות מגיש - כללי

ברובד השירות לקוחות תשתית המיסור תיתמך על ידי צוותי הפיתוח (דרג ג) של המגיש. הספקים ייתמכו ראשונית על ידי שירות לקוחות דרג א בליווי הסלמת אירוע לדרג ב במקרה הצורך (ואף לדרג ג). בנוסף אירועי הטמעה והדרכה ילוו על ידי דרג ב. צוות שירות הלקוחות דרג א של המגיש יעמוד בקשר ישיר עם צוות שירות לקוחות דרג א של משהב"ט שייתמך על ידי דרג ב ו-ג במקרה הצורך. צוותי העבודה של אגף התיקשוב אשר מעורבים בתהליכי העבודה מול הספקים ואשר יש צורך בקשר בינם לבין המגיש ייתמכו על ידי מנהל לקוחות בפן העיסקי, ועל ידי מנהל פרויקטים בפן התיפעולי.

#### 4.1.1 מרכז תמיכה – Helpdesk (Call Center)

שעות פעילות נדרשות:

07:30-19:00 בימים א-ה שהם ימי חול.

07:30-12:30 בערבי שבת וערבי חג.

החל מהשעה 19:00 יש להעמיד תורן לצורך מענה לתקלות משביתות.

#### 4.1.2 צוות שירות דרג א מגיש

צוות שירות לקוחות של המגיש אשר אמון על הקשר לספקי המשרד מצד אחד ולצוות שירות לקוחות של המשרד.

הצוות אמור להתמקצע בתקלות טכניות במערכות המיסור של המגיש, בתוכנות הסוכן שיושבות במשרד ובתוכנות הסוכן\ אמצעי ההעברה אצל ספקי המשרד.

נושאי טיפול צוות:

1. תמיכה טלפונית שוטפת לספקים.
2. מענה לפניות דוא"ל או פורטל.
3. מענה לשאלות בתיפעול הפורטל לספקים.
4. טיפול בתקלות ראשוניות קלות ע"י התחברות מרחוק לתחנות הקצה של הספקים.

#### 4.1.3 צוות שירות דרג ב' מגיש

צוות שירות של מומחי יישום ומטמיעים של המגיש אשר אמון על פתרון תקלות יישום מתקדמות וכן על הקשר לספקי המשרד בהיבט של הטמעה, התקנת תוכנות ופתרון בעיות תוכנה.

נושאי טיפול צוות:

1. תמיכה בשלבי החיבור הראשוני וההגדרה של המערכת לספקים.
2. הדרכה טלפונית.
3. הדרכה באתר הספק, אם יש צורך.
4. תמיכה ברמת אפיון המוצר.
5. טיפול התקלות על ידי התחברות אל תחנת הקצה של הספק.

#### 4.1.4 צוות שירות דרג ג מגיש

צוות של תכניתנים\מפתחים\מיישמים אשר אמונים על פיתוח מערכות המיסור המרכזית של המגיש וכן על תוכנות לוייניות אחרות אשר בשימוש המשרד ו\או ספקי המשרד.

תפקיד הצוות הינו פיתוח רכיבים החסרים במערכות המיסור המרכזיות של המגיש על מנת לתמוך בפורמטים, צרכים מיוחדים של ספקי המשרד.

נושאי טיפול צוות:

1. תמיכה ברמת תכנות המוצר.
2. תחזוקת המערכת.
3. ביצוע עדכוני גרסא.

#### 4.1.5 מנהל פרויקט מגיש

איש ניהול פרויקטים בעל רקע של עבודה בתחום הפיתוח (רצוי מתחום ה-B2B), בעל ניסיון של לפחות 5 שנים בתחום הפיתוח או ניהול הפרויקטים לפני כניסתו לתפקיד, אשר יהיה אמון על הקשר מול צוות המיסור של אגף מל"ן במשרד.

#### 4.1.6 מנהל לקוח מגיש

איש שימור לקוחות אשר אמון על הקשר מול גורמי המשרד הבאים: צוות רכש במנה"ר, צוות מיסור, רכש, פיננסי ולוגיסטי במל"ן.

איש זה אמון על הנושאים העסקיים, הבירוקרטיים והלוגיסטיים שבקשר שבין המשרד לבין המגיש.

### 4.2 תפעול שוטף

#### 4.2.0 השבתות מערכות מגיש

בכל השבתה מתוכננת של מערכת שלמה או חלקי מערכת שמשפיעה על התהליכים שבין המשרד לבין ספקי המשרד, יש לבצע תיאום השבתה מול הצוות שיוגדר כאחראי לנושא במשהב"ט. מול הצוות הזה יעמוד מנהל פרוייקט מטעם המגיש. נדרשת יכולת התראה במייל לרשימת נמענים מבוקשת מראש על ידי משהב"ט.

בכל השבתה או תחזוקה שיש בה להשפיע על הפעילות יש להתריע לפחות 5 ימי עסקים לפני מועד שיבוש הפעילות.

#### 4.2.1 השעיית עבודה מול ספק

היה וכתוצאה מגורמים הקשורים ביחסים העיסקיים שבין המגיש לספק, החליט המגיש להפעיל סנקציה על פעילות הספק שתשפיע על פעילותו מול משהב"ט, יש לאפשר לספק תקופת התארגנות של לפחות 30 ימי עסקים לצורך מעבר למגיש אחר מבלי לפגוע בפעילותו מול המשרד. נדרשת יכולת התראה במייל לרשימת נמענים מבוקשת מראש על ידי משהב"ט.

ככל שהספק לא עמד בהוראות סעיף זה, משהב"ט שומר לעצמו את הזכות לחילוט הערבות כולה או חלקה בהתאם לשיקול דעתו הבלעדי (כמפורט בסעיף 1.2.0).

#### 4.2.2 הכנסת ספק חדש\ספק עובר

מרגע ההודעה על הצטרפות ספק חדש לשירותי המפעיל (חתימת ההסכם בין המפעיל לספק), על המפעיל להיערך תוך חמישה ימי עסקים להיות מוכן תפעולית לעבודה בייצור מול הספק שהצטרף.

כאשר מדובר בספק שעובר בין מפעילים, על המפעיל הקולט להיערך תוך 20 ימי עסקים להיות מוכן תיפעולית בייצור עבור הספק העובר. על המפעיל הקולט להיערך לביצוע קליטת נתוני מסרים מהמפעיל הקודם: כל המסרים שאינם בסטטוס סופי ללא קשר לתאריך כתיבתם במאגר הנתונים, וכן מסרים שבסטטוס סופי של כחצי שנה אחורה. נדרש תיאום בין המפעיל הקולט לבין המפעיל הקודם לגבי תצורת העברת המידע בשני המקרים. על המפעיל המשחרר להיערך תוך 15 ימי עסקים להעברת הנתונים הללו. פעולת העברת הנתונים תתבצע על ידי הוצאת הנתונים בפורמט מבנה המסר כפי שמוגדר על ידי משהב"ט. כלומר המפעיל המעביר את הנתונים מחוייב להוציא את הנתונים בקבצים הבנויים במבנה המקורי כפי שנכנס אליהם ממשהב"ט.

לאחר ביצוע טיוב נתונים מוצלח על המפעיל החדש לאשר למפעיל הישן למחוק את הנתונים, שרק אז יוכל לבצע את המחיקה בפועל.

על המפעיל הקולט לנהל את המעבר של הספק באופן כזה שלא ייגרם לו נזק כספי. מכיון שמשהב"ט דורש מהספקים להצהיר באתר האינטרנט על המפעיל עימו הוא עובד כתנאי לעבודה דיגיטאלית, יהיה על המפעיל להיות מתואם מול הספק גם בהיבט הזה. לצורך העניין על המפעיל הקולט והספק העובר לדאוג שבלילה הקודם ליום המעבר בפועל ישונה קוד המפעיל המוצהר באתרי האינטרנט של המשרד.

לאחר סיום העברה תקין ואישור המפעיל הקולט על המפעיל הקודם חובה למחוק את נתוני הספק שעבר ממערכות המידע שלו.

ככל שהספק לא עמד בהוראות סעיף זה, משהב"ט שומר לעצמו את הזכות לחילוט הערבות כולה או חלקה בהתאם לשיקול דעתו הבלעדי (כמפורט בסעיף 1.2.0).

#### 4.2.3 שירות התקנה הדרכה והטמעה

על המגיש לספק שירותי הדרכה והטמעה ככל שיידרשו על ידי ספק המשרד, אם בשלב כניסתו כספק חדש ואם בשלב אחר, כתוצאה משינוי שבוצע במערכות המגיש או שינוי שבוצע במערכות או בצוותי המשתמשים של ספק המשרד. שירות זה כולל גם התקנת תוכנות או הטמעות באתר ספק המשרד.

### 4.3 אמנת שירות - SLA

#### על מנת להבטיח את איכות השירות הניתן לספקי משרד הביטחון, ימדד מפעיל קד"ם רבעונית ושנתית על איכות השירות כמפורט להלן:

#### 4.3.0 מדידת תקלות מיסור מערכתיות.

בטבלה הבאה מפורטות סוגי תקלות המחייבות את המגיש בניקוד. הניקוד נזקף לחובת המפעיל בכל פעם שקרתה תקלה מהסוג המצויין. הניקוד הינו ניקוד נצבר כך שבקרות מספר תקלות, ייזקף לחובתו של המפעיל סכום הניקוד עבור אותן תקלות.

הניקוד נצבר רבעונית ושנתית, ומקבל התייחסות שיפוטית בסוף כל רבעון ובסוף כל שנה.

| **סעיף** | **סוג התקלה** | **משך הזמן המקסימלי עד להתחלת הטיפול בתקלה** | **ניקוד** |
| --- | --- | --- | --- |
|  | תקלה שמשביתה את כל אתר המגיש או שמשביתה את מערכת המגיש באופן שאין תעבורה של מסרים אל\ממשהב"ט לחלוטין של למעלה מחצי שעה | מיידי עם קבלת הדיווח/גילוי תקלה ע"י המפעיל | 100 |
|  | אי עמידה בביצוע סקרי אבטחת מידע כפי שמפורט בסעיף 3.2.10 |  | 100 |
|  | אי עמידה בביצוע תיקון ליקויי אבטחת מידע כפע שמתואר בסעיף 3.2.11 |  | 100 |
|  | תקלה שגורמת לאי זרימה כוללת של פקודות עבודה לספקים של למעלה משעה | מיידי עם קבלת הדיווח/גילוי תקלה ע"י המפעיל | 60 |
|  | תקלה שגורמת לאי זרימה כוללת של מרשמים רפואיים לספקים של למעלה משעה | מיידי עם קבלת הדיווח/גילוי תקלה ע"י המפעיל | 50 |
|  | תקלה המונעת זרימת פק"עות לספק ספציפי של למעלה משעה | מיידי עם קבלת הדיווח/גילוי תקלה ע"י המפעיל | 45 |
|  | תקלה המונעת זרימת מרשמים רפואיים לספק ספציפי של למעלה משעה | מיידי עם קבלת הדיווח/גילוי תקלה ע"י המפעיל | 40 |
|  | תקלה שגורמת לאי זרימה כוללת של פקודות אספקה לספקים של למעלה משלוש שעות | עד ארבע שעות מרגע קבלת הדיווח/גילוי תקלה ע"י המפעיל | 35 |
|  | תקלה שגורמת לאי זרימה כוללת של אישור ספק לפקודת עבודה לספקים של למעלה משלוש שעות | עד ארבע שעות מרגע קבלת הדיווח/גילוי תקלה ע"י המפעיל | 30 |
|  | תקלה שגורמת לאי זרימה כוללת של חשבוניות למשהב"ט של למעלה משלוש שעות | עד ארבע שעות מרגע קבלת הדיווח/גילוי תקלה ע"י המפעיל | 20 |
|  | אי עמידה בסעיף 4.2.2 הכנסת ספק חדש (הן לגבי מפעיל פולט והן לגבי מפעיל קולט) |  | 10 |
|  | תקלה שגורמת לאי שליחת מסרים כוללת מסוגים שלא צוינו בסעיפים 2-6 של למעלה משלוש שעות | עד ארבע שעות מרגע קבלת הדיווח/גילוי תקלה ע"י המפעיל | 10 |
|  | תקלה המונעת מספק ספציפי תעבורת נתונים(למעט פק"ע או מרשמים רפואיים) של למעלה משלוש שעות | 24 שעות מרגע קבלת הדיווח/גילוי תקלה ע"י המפעיל | 6 |
|  | תקלה המונעת זרימת פק"אות לספק ספציפי של למעלה משלוש שעות | 24 שעות מרגע קבלת הדיווח/גילוי תקלה ע"י המפעיל | 5 |
|  | תקלה המונעת זרימת אישור לספק על פק"ע לספק ספציפי של למעלה משלוש שעות | 24 שעות מרגע קבלת הדיווח/גילוי תקלה ע"י המפעיל | 4 |
|  | תקלה המונעת מספק ספציפי יכולת לשלוח או לקבל סוג מסר אחר משצויין בסעיפים 9-12 של למעלה מארבע שעות | 24 שעות מרגע קבלת הדיווח/גילוי תקלה ע"י המפעיל | 1 |
|  |  |  |  |

משהב"ט שומר לעצמו את הזכות לשנות את משך הזמן לטיפול בתקלות מיסור ספציפיות בהתאם לצרכים המבצעיים.

#### 4.3.1 תוצאות השיפוט הרבעוני.

מפעיל אשר צבר מעל 150 נקודות ברבעון:

המשרד שומר לעצמו את הזכות לבטל לספק את סיווג מורשה קד"ם (כאמור בסעיף 1.5.0)

ו/או לחלט את הערבות שלו כולה או חלקה בהתאם לשיקול דעתו הבלעדי (כמפורט בסעיף 1.2.0).

וזאת לאחר מתן התרעה בכתב של 30 ימים טרם הביצוע.

#### 4.3.2 תוצאות השיפוט השנתי.

מפעיל אשר צבר מעל 450 נקודות בשנה:

המשרד שומר לעצמו את הזכות לבטל לספק את סיווג מורשה קד"ם (כאמור בסעיף 1.5.0)

ו/או לחלט את הערבות שלו כולה או חלקה בהתאם לשיקול דעתו הבלעדי (כמפורט בסעיף 1.2.0).

וזאת לאחר מתן התרעה בכתב של 30 ימים טרם הביצוע.

### 4.4 בקרה על תיפעול המערכת ורמת השירות

#### 4.4.0 מודל הבקרה

1. המגיש יעביר דיווח חודשי על פעילות המערכת לגורם אשר יתבקש על ידי משהב"ט.
2. הדיווחים החודשיים יכללו:

1. עמידת המגיש בסעיפים הנקובים ב-SLA.

2. רמת שירות: מספר פניות למוקד, תלונות שהגיעו למוקד הספק

3. תקלות במערכת ודרך פיתרונן ותיקונן

4. השבתות והחזרה לשירות

5. שידרוגים מתוכננים

6. שידרוגים שבוצעו

7. דיווח על אירועי אבטחת מידע חריגים

8. דיווח על כל אירוע חריג מיוחד ודרך הטיפול בו

9. דו"ח מרכז תקופתי על כל סוג הפרה המנויה בסעיף 4.3

1. אירועים חריגים הדורשים התייחסות מיידית, ידווחו לאלתר לגורם אשר ימונה מטעם משהב"ט.
2. משהב"ט שומר לעצמו את הזכות לזמן דיון סטטוס חודשי או במרווח אחר באם יידרש.
3. יש להגיש את הדיוחים בקובץ אקסל.

#### 4.4.1 הגורם המבקר

1. המשרד יהיה רשאי למנות גורם מטעמו שיבצע בקרה על המערכת ותיפעולה, כולל רמת השירות והיקפה. על הספק לשתף פעולה עם הגורם הן ביחס במהלך הביקורת והן בקיום מסקנותיה.
2. במקביל לבקרה דלעיל, ייקבע כמתחייב מהוראות החוקים אליו כפופים השירותים הנדרשים במסמך זה, כפי שיהיו מעת לעת גורם המבקר את רמת אבטחת המידע של המערכת, ועמידת הספק בהתחייבויותיו.
3. משהב"ט שומר לעצמו את הזכות לזמן דיון סטטוס חודשי או במרווח אחר באם יידרש.

## נספחים

### נספח א: מודל סביבת מפעילים (סעיף 2.2.1)

שירות דרג ג'

שירות דרג ב'

שירות דרג א'

**ספקים**

שירות הקלדה(עתידי)

שירות סריקה(עתידי)

שירות פורטל

שירות B2B

תשתית המיסור

**מערכות המיסור משהב"ט(צוות מיסור)**

שירות דוחות

מנהל פרויקט

מנהל לקוח

ניטור תשתיתיתי

ניטור עיסקי

תוכנת סוכן\לקוח

**תשתית אבטחת מידע**

תוכנת סוכן\לקוח

### נספח ב: מסמך אישור כללי

**לכבוד**

**משרד הביטחון**

**אגף תיקשוב**

**הנדון: הגשת בקשה לסיווג כספק קשר דיגיטלי מסחרי**

יש למלא כל פרטי הטופס ולחתום במקום המיועד

|  |  |
| --- | --- |
| שם המגיש |  |
| כתובת |  |
| טלפון |  |
| פקס |  |
| איש הקשר |  |
| מס' ספק (ככל וקיים) |  |
| תאריך |  |

1. **אני הח"מ \_\_\_\_\_\_\_\_\_\_\_\_מס' חברה \_\_\_\_\_\_\_\_\_\_\_\_\_שכתובתנו היא \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, מצהירים, מסכימים ומתחייבים בזה כלפיכם כדלקמן:**

קראנו בעיון את מסמך אפיון הדרישות לסיווג ספק מורשה לקשר דיגיטלי מסחרי (להלן: "קד"ם"), על כל נספחיו (להלן: "מסמכי האפיון").

הננו מצהירים, כי הבנו את כל מסמכי האפיון על כל פרטיהם, ובחנו את כל התנאים והנסיבות הקשורים בסיווג כספק קד"ם ו/או הנובעים ממנו, וכן את כל הגורמים האחרים הרלבנטיים והעשויים להשפיע על הבנת פעילות ספק קד"ם ועל קיום כל ההתחייבויות הכלולות במסמכי האפיון.

* + 1. בהתאם לכל האמור לעיל, ולאחר שבחנו בחינה זהירה ומדוקדקת את כל תנאי ומסמכי האפיון האמורים, הננו מגישים בקשתנו זו לסיווג כספקי קד"ם והרינו מתחייבים בזה, אם נקבל הסיווג, לבצע ולקיים את כל ההתחייבויות הכלולות במסמכי האפיון.

1. הננו מצהירים כי אנו בעלי ידע וניסיון ובעלי יכולת ארגונית, מקצועית וכספית בנושא קד"ם, וכי הננו עומדים בכל תנאי הניסיון המוקדם שפורטו באפיון, לרבות:
2. ניסיון של לפחות 5 שנים בשירותים המוצעים.
3. היקף לקוחות העולה על 1,000 לקוחות המעבירים מסרים באופן שוטף
4. היקף פעילות העולה על 20000 מסרים ביום ועל 1 GB ביום
5. יכולת העברת מידע של לפחות 100,000 מסרים ליום ולמסרים של לפחות 2 GB.
6. במידה ונקבל סיווג כספק קד"ם, אנו מתחייבים לבצע את כל השירותים המפורטים במסמכי האפיון ולרבות:
7. יישום תהליכי ה-B2B המתוארים
8. פיתוח האתר לשירות הספקים
9. יישום דרישות התשתית ואבטחת המידע
10. עמידה ב-SLA ובסטנדרטים של השירות לקוחות הנדרשים
11. במידה ונקבל סיווג כספק קד"ם, הרינו מתחייבים בזה כלפיכם, לבצע את כל הפעולות הנדרשות כלפי משהב"ט וכלפי הספקים, בהתאם למועדים הנקובים במסמכי האפיון ובכללם:
12. אחזקת מסרים בסטטוס סופי למשך שנה אחורה, באופן המאפשר אחזור המסרים על ידי כל ספק את מסריו, ועל ידי המשרד לגבי כלל הספקים.
13. להציג כל נתון שיידרש על ידי המשרד.
14. לאפשר גישה לאתרינו באם יידרש בכל עת.
15. עמידה בכל הדרישות העולות ממסמך זה ואשר נדרשות גם במהלך התקופה בה אנחנו ניתן שירות למשהב"ט כבעלי סיווג ספק קד"ם.
16. נקבל עלינו את השינויים אשר יידרשו מעת לעת, כתוצאה מדרישות מערכת הביטחון, למסמך זה.
17. במידה ונקבל סיווג קד"ם אנחנו מבינים ומסכימים כי אי עמידה בדרישות המסמך ובשינויים שלו מעת לעת יכולים לגרור, על פי החלטת משהב"ט, ביצוע של חילוט ערבות,כולה או חלקה ו\או השעייה או אף ביטול הסיווג שניתן לנו כספק לתת שירותי קד"ם לספקי המשרד.
18. חתימה על נספח זה תהיה תקפה אך ורק בכפוף לחתימה בסוף כל אחד מהפרקים 1-4 של המסמך.

ובאנו על החתום (מורשי החתימה מטעם החברה):

מנכ"ל החברה(או נציג מטעמו): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

כתובת:\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

תאריך:\_\_\_\_\_\_\_\_\_\_\_\_\_\_ -------------------

חתימת המציע

(חתימה וחותמת)

-------------------------------------------------------------------------------------

### נספח ג: מסמך אישור תהליכים (סעיף 2.5)

רשימת תהליכים

אני הח"מ \_\_\_\_\_\_\_\_\_\_\_ בתפקידי כ\_\_\_\_\_\_\_\_\_\_\_ בחברת \_\_\_\_\_\_\_ (להלן: "המגיש") מתחייב, כי ביכולת המגיש להציע את התהליכים המפורטים בטבלה לספקי משהב"ט, וכן, כי נציג משהב"ט יוכל לצפות בתהליכים מעמדת המשתמש הממוקמת במשרד הביטחון:

| סעיף | שם | חתימת הח"מ כי השירות מוצע ע"י המגיש |
| --- | --- | --- |
| 2.5.1 | שמירת נתון סוג מערכת |  |
| 2.5.2 | ריבוי מספרי ספק לגורם עיסקי אחד |  |
| 2.5.3 | שליחת הזמנת רכש למפעיל |  |
| 2.5.4 | שליחת מסר מחירון מרק"ט\נתיבים |  |
| 2.5.5 | שליחת פקודת אספקה(פק"א) מרק"ט לספק |  |
| 2.5.6 | קבלת אישור לפקודת אספקה מרק"ט מהספק |  |
| 2.5.7 | קבלת תעודת משלוח מהספק |  |
| 2.5.8 | שליחת אישור על תעודת משלוח לספק |  |
| 2.5.9 | שליחת דיווח קבלה לספק |  |
| 2.5.10 | שליחת פקודת עבודה(פק"ע) לספק |  |
| 2.5.11 | קבלת אישור לפק"ע מהספק |  |
| 2.5.12 | קבלת גיליון שירות מהספק |  |
| 2.5.13 | קבלת נתוני GPS עבור גיליון שירות מהספק |  |
| 2.5.14 | שליחת אישור על גיליון שירות לספק |  |
| 2.5.15 | שליחת תחשיב לתשלום לספק |  |
| 2.5.16 | קבלת חשבונית לוגיסטית מהספק ע"ס הזמנת רכש |  |
| 2.5.17 | קבלת חשבונית לוגיסטית נתיבים מהספק |  |
| 2.5.18 | קבלת חשבונית לוגיסטית מרק"ט מהספק |  |
| 2.5.19 | שליחת סטאטוס חשבונית לספק |  |
| 2.5.20 | שליחת הודעת זיכוי לספק |  |
|  |  |  |

### נספח ד: מסמך אישור תוכנת סוכן (סעיף 3.1)

תוכנת סוכן

אני הח"מ \_\_\_\_\_\_\_\_\_\_\_ בתפקידי כ\_\_\_\_\_\_\_\_\_\_\_ בחברת \_\_\_\_\_\_\_ (להלן: "המגיש") מתחייב, התקנת תוכנת סוכן במשרד הביטחון, וכן, כי תוכנת הסוכן תכיל את השירותים כמפורט להן:

| סעיף | שם | חתימת הח"מ כי השירות מוצע ע"י המגיש |
| --- | --- | --- |
| 3.1.1 | אחסנת נתונים מרכזית |  |
| 3.1.2 | מערכת הפעלה |  |
| 3.1.3 | כלי פיתוח ותחזוקה |  |
| 3.1.4 | כלי תפעול וייצור |  |
| 3.1.5 | כלי שליטה ובקרה למנהל המערכת |  |
| 3.1.6 | עומסים וביצועים |  |
| 3.1.7 | אבטחת מידע |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### נספח ה: מסמך אישור אבטחת מידע (סעיף 3.2)

אבטחת מידע

ראה קובץ אקסל מצורף "דרישות אבטחה לספקים – קדם"

### נספח ו: תצהיר PCI-DSS (סעיף 1.4.2)

ת צ ה י ר

אני הח"מ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ת.ז מס'\_\_\_\_\_\_\_\_\_\_\_\_\_\_, המשמש כ\_\_\_\_\_\_\_\_\_\_\_ בחברת \_\_\_\_\_\_\_\_, ח.פ. \_\_\_\_\_\_\_\_\_\_\_ (להלן: "החברה"), לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר בזה בכתב כדלקמן:

1. בתוקף תפקידי זה הנני מוסמך להצהיר כאמור בהצהרה זו.
2. הנני מצהיר כי מערכת גביית התשלומים בכרטיסי אשראי המשמשת את החברה עומדת בכל דרישות מועצת חברות כרטיסי האשראי (מועצת PCI), לרבות תקן PCI-DSS.
3. הנני מצהיר כי לחברה אישור מגוף QSA מוסמך, וכי ביכולתי להציגו למשרד הביטחון לפי בקשה מפורשת.
4. הנני מצהיר כי מערכת גביית התשלומים בכרטיסי אשראי המשמשת את החברה עומדת בכל דרישות חברות האשראי הישראליות (חברת CAL, קבוצת ישראכרט אמריקן אקספרס ולאומי קארד), ככל שישנן.

זהו שמי זאת חתימתי וכל הצהרותיי כפי שניתנו בגוף התצהיר ו/או בחלק מנספחיו ו/או בכל נספחיו ו/או חלק מחלקיו, הינן אמת לאמיתה.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

חתימה

א י ש ו ר

אני הח"מ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, עו"ד, מאשר/ת בזה כי ביום \_\_\_\_\_\_\_\_\_\_\_\_ התייצב בפני מר \_\_\_\_\_\_\_\_\_\_\_\_\_ אשר הזדהה בפני עם ת.ז. מס' \_\_\_\_\_\_\_\_\_\_\_\_ (המוכר לי אישית) ולאחר שהזהרתיו כי עליו להצהיר את האמת וכי אם לא יעשה כן יהיה צפוי לעונשים הקבועים בחוק, אישר את נכונות הצהרתו הנ"ל וחתם עליה בפני.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

חותמת חותמת

### נספח ז: כתב ערבות (סעיף 1.2.0)

**תאריך--------**

**לכבוד:**

**משרד הביטחון/אגף הכספים**

**הקריה, תל-אביב**

**הנדון: ערבות בנקאית/ כתב ערבות חברת ביטוח בלתי מותנית מס'**

1. על פי בקשת \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (להלן "המבקש") אנו ערבים בזאת כלפיכם לתשלום כל סכום, לפי דרישתכם, עד לסכום כולל של 50,000₪ (חמישים אלף ש"ח) (להלן- "סכום הערבות") צמוד למדד לפי האמור בסעיף 2 להלן, בקשר להשתתפות המבקש כמפעיל מורשה לקשר דיגיטלי מסחרי למשרד הבטחון.

2. סכום הערבות יהיה צמוד למדד המחירים לצרכן כפי שהוא מתפרסם מפעם לפעם על-ידי הלשכה המרכזית לסטטיסטיקה ולמחקר כלכלי, בתנאי ההצמדה כמפורט להלן: אם יתברר ביום התשלום על-פי דרישתכם כי המדד הקובע עלה לעומת המדד הבסיסי, נשלם את סכום הערבות כשהוא מוגדל בשיעור העלייה של המדד הקובע לעומת המדד הבסיסי. אם יתברר ביום התשלום על-פי דרישתכם כי המדד הקובע ירד לעומת המדד הבסיסי, נשלם לכם את אותו סכום הנקוב בדרישתכם, ובתנאי שלא יעלה על סכום הערבות.

בכתב ערבות זה:

"מדד קובע" - המדד שפורסם לאחרונה לפני התשלום בפועל על-פי ערבות זו.

"מדד בסיס" - המדד שפורסם בגין **חודש 12/2013.**

3. לפי דרישתכם הראשונה בכתב, אנו נשלם לכם כל סכום הנקוב בדרישה ובלבד שלא יעלה על סכום הערבות, בתוספת הפרשי הצמדה כאמור לעיל, תוך 7 ימים מקבלת דרישתכם הראשונה בכתב, מבלי להטיל עליכם חובה לבסס או לנמק את דרישתכם או לדרוש תחילה את התשלום מאת המבקש.

4. ערבות זו תהיה בתוקף עד יום **-------** ועד בכלל. כל דרישה מצדכם לתשלום סכום הערבות צריכה להגיע בכתב למשרדי הסניף החתום מטה שכתובתו הינה \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ לא יאוחר מאשר התאריך הנ"ל.

5. מודגש בזה כי "דרישה בכתב" אינה כוללת דרישה באמצעות פקסימיליה, מברק או כל אמצעי אלקטרוני אחר.

6. ערבות זו אינה ניתנת להעברה.

**בכבוד רב,**

**בנק/חברת ביטוח :**

### נספח ח: מסמך אישור תיפעול שוטף(סעיף 4.2)

רשימת שירותים

אני הח"מ \_\_\_\_\_\_\_\_\_\_\_ בתפקידי כ\_\_\_\_\_\_\_\_\_\_\_ בחברת \_\_\_\_\_\_\_ (להלן: "המגיש") מתחייב, כי המגיש יקיים את הדרישות המוצגות בסעיפים המפורטים בטבלה לספקי משהב"ט:

| סעיף | שם | חתימת הח"מ כי השירות יבוצע במלואו כלשון הסעיף ע"י המגיש |
| --- | --- | --- |
| 4.2.0 | השבתות מערכות מגיש |  |
| 4.2.1 | השעיית עבודה מול ספק |  |
| 4.2.2 | הכנסת ספק חדש\ספק עובר |  |
| 4.2.3 | שירות התקנה הדרכה והטמעה |  |
| 4.4.0 | מודל הבקרה |  |
| 4.4.1 | הגורם המבקר |  |
|  |  |  |
|  |  |  |
|  |  |  |

### נספח ט: סרגל מבנה מסר הזמנה (סעיף 2.5.1)

ראה קובץ מצורף "ממשק הזמנה יוצא למפעילים"

### נספח י: סרגל מבנה פקודת עבודה (סעיף 2.5.10)

ראה קובץ מצורף "מסמך איפיון מערכת נתיבים מפעילים"

סעיפים רלוונטיים: 5, 14א

### נספח יא: סרגל מבנה אישור על פקודת עבודה (סעיף 2.5.11)

ראה קובץ מצורף "מסמך איפיון מערכת נתיבים מפעילים".

סעיפים רלוונטיים: 6, 14ב

### נספח יב: סרגל מבנה גיליון שירות(סעיף 2.5.12)

ראה קובץ מצורף "מסמך איפיון מערכת נתיבים מפעילים".

סעיפים רלוונטיים: 7, 14ג

### נספח יג: סרגל מבנה תחשיב לתשלום (סעיף 2.5.12)

ראה קובץ מצורף "מסמך איפיון מערכת נתיבים מפעילים".

סעיפים רלוונטיים: 8, 14ד

### נספח יד: סרגל מבנה קבלת חשבונית לוגיסטית מהספק ע"ס הזמנת רכש (סעיף 2.5.16)

ראה קובץ "מסמך הסבר מסר תמש" אשר בתוכו פירוט של מסמכי המשנה הרלוונטיים.

### נספח טו: סרגל מבנה חשבונית לוגיסטית נתיבים(סעיף 2.5.17)

ראה קובץ מצורף "מסמך איפיון מערכת נתיבים מפעילים".

סעיפים רלוונטיים: 9, 14ה

### נספח טז: סרגל סטאטוס חשבונית(סעיף 2.5.18)

ראה קובץ מצורף "מסמך אפיון מסר סטטוס חשבונית"

### נספח יז: סרגל מבנה הודעת זיכוי (סעיף 2.5.19)

ראה קובץ מצורף "מסמך אפיון מסר הודעת זיכוי"

### נספח יח: איפיון אלגוריתם ספק מקבל המסר

ישנם ספקים המהווים בתי תוכנה שנותנים שרותים מיוחדים לספקי משהב"ט. ספקים אלו שולחים את מסרי החשבוניות עבור ספקי משהב"ט להם הם נותנים שרות. ומקבלים את הסטטוסים עבור ספקי משהב"ט להם הם נותנים שרות. את השידוך בין ספק בית התוכנה לספק משהב"ט מבצעות מערכות המיחשוב של משהב"ט, כאשר על פי הקונבנציה שנבנתה המגיש יבצע את ההחלטה לאיזה ספק לשלוח על בסיס נתון שמופיע בשם הקובץ. הוחלט שלפני סיומת הקובץ באמצעות קו תחתון מפריד יופיע מספר הספק אליו יש לשלוח בפועל את המסר.

לדוגמא(ההדגמה מתבצעת על מסר סטאטוס חשבונית אך רלוונטית לכל סוגי המסרים בהם מיושמת השיטה):

M12\_Heshbonit\_<Real Supplier Number><InvoiceId><InvoiceDate><StatusDate><StatusTime><StatusCode><StatusSever>\_<msg creation date><msg creation time>\_<ModOriginalSystem>\_<environment>\_<receiver supplier>.xml

כאשר receiver supplier הינו הספק שבפועל אמור לקבל את המסר.

M12\_Heshbonit\_00833301311201105252011110611260216S\_20111106220207\_000\_0000000021161805\_S400\_0083330222.xml

במקרה הזה רואים שסטטוס החשבונית שייך לספק 0083330131 אבל צריך להישלח בפועל לספק 0083330222

### נספח יט: תרשים אוביקטים (סעיף 2.15.4)

תעודת משלוח

תעודת משלוח

הזמנה

פק"א

פק"ע

תעודת משלוח

גיליון שירות

תחשיב לתשלום

דיווח קבלה\תחשיב לתשלום

חשבונית

הודעת זיכוי

חשבונית

הודעת זיכוי

### נספח כ' – שמירה על סודיות עסקית

1. הגדרות-
2. **"המידע**" - משמעו כל מידע שהתקבל מספקי המשרד לצורך קבלת השירות, הכולל בין היתר הזמנות, חשבוניות, הסכמים, מידע סטטיסטי, נתוני מידע גאוגרפי ועוד.
3. **"השירות"** – משמעו הספקת פלטפורמה דיגיטאלית למסחר אלקטרוני לספקי המשרד בהתאם לכלל הדרישות שהוגדרו במסמך האפיון קד"מ.
4. **"מפעיל"** – כהגדרתו במסמך האפיון קד"מ, לרבות עובדיו או מי מטעמו.
5. **"המשרד"** – משרד הביטחון ויחידות הסמך שלו.
6. **"מוסר המידע"** – ספק של משרד המקבלים שירות מהמפעיל.
7. נספח זה הינו חלק בלתי נפרד ממסמך האפיון קד"מ.
8. לאור רגישות המידע הנמסר ע"י מוסר המידע למפעיל, אשר כולו או חלקו מהווה סוד עסקי של מוסר המידע, חשיפתו לגורמים מתחרים של מוסר המידע עלולה לגרום לו לנזק כלכלי ותדמיתי רב, לכן מתחייב ומצהיר המפעיל כדלקמן;
9. לשמור על סודיות המידע שיימסר לו ע"י מוסר המידע, לאורך כל תקופת מתן השירות ולאחריו.
10. לא להפיץ את המידע, לא להעבירו ולא לגלותו לאחרים, ללא קבלת אישור מוקדם לכך מאת מוסר המידע, אלא לצורך מתן השירות.
11. לא לעשות במידע או בחלקו כל שימוש פרט לצורך מתן השירות.
12. לא לעשות שום העתקים מהמידע למעט העתקים שיבוצעו באישור המזמין לצורך אספקת השירות.
13. ביום סיום מתן השירות, על המפעיל להחזיר לידי מוסר המידע את כל המידע שברשותו שהתקבל ע"י מוסר המידע או להשמידו לאלתר, בהתאם לעניין.
14. המפעיל מצהיר שהובהר לו כי הפרת של הוראות סעיף 2 לעיל הינן מעיקרי מסמך אפיון קד"מ. הפר המפעיל הוראות אילו, כולן או חלקן, המשרד שמור לעצמו את הזכות, בהתאם לשיקול דעתו הבלעדי, לבחור באחד או יותר מהפעולות הבאות;
15. השהיית סיווג קד"מ למפעיל או ביטולו.
16. חילוט הערבות הבנקאית שנתן המפעיל לעניין סיווג קד"מ, כולה או חלקה.
17. העלאת המפעיל לוועדת להשהיית ספקים של משרד הביטחון, לצורך קבלת החלטה על המשך היותו ספק מאושר של משרד הביטחון.
18. לתבוע כל סעד אחר בהתאם להוראות הדין או נספח זה.
19. המפעיל מתחייב לפצות ו/או לשפות את המשרד בגין כל נזק ו/או הוצאה שתיגרם לו, לרבות עקב תביעת צד ג', כתוצאה מהסתמכות המשרד על הצהרות המפעיל בנספח זה.
20. מבלי לגרוע מאחריות המפעיל על פי נספח זה ו/או על פי כל דין, להבטחת התחייבויותיו, מתחייב המפעיל, לערוך ולקיים על חשבונו בחברת ביטוח מורשית, ביטוח **אחריות מקצועית** בגבולות אחריות נאותים כאשר משרד הביטחון יתווסף כמבוטח נוסף ובפוליסה ייכלל סעיף ויתור על זכות תחלוף כלפי משרד הביטחון.

**אני \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , מורשה חתימה של חברת \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**מצהיר ומתחייב בשם החברה למלא אחר הוראות נספח זה במלואם.**

**חותמת וחתימה\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ תאריך\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

### נספח כא' – תיאור תהליך קבלת הסיווג

להלן מתואר עיקרי התהליך שעל המגיש לעבור על מנת לקבל את סיווג ספק מורשה קד"ם.

1. תנאי ראשוני לתהליך האישור הינו בדיקה שהספק הינו ספק מאושר של מנה"ר במשהב"ט בעל מספר ספק מונפק. למגיש שאינו ספק משהב"ט יש להסדיר זאת ביחידת הספקים של מנה"ר על פי נהלי המשרד.
2. לאחר קבלת מספר ספק, תתקיים פגישה במשרדי משרד הביטחון לצורך היכרות עם המגיש, פועלו ,עסקיו , קרבתו לתחום העיסוק הנדרש בקד"ם ואנשי המפתח הפועלים באירגונו.
3. תבוצע בדיקת נאותות לספק כדי לוודא שהספק עומד מבחינה משפטית ועיסקית בדרישות קד"מ.
4. הגשת מענה לכל הדרישות בדגש על חתימה על נספח ב'. ללא חתימה על נספח זה שתועבר למשרד לא תהיה התקדמות בתהליך.
5. עמידה בפרק אבטחת מידע (סעיף 3.2)
   1. יש לבצע את התאמות המערכות של המגיש לדרישות אבטחת המידע המפורטות במסמך דרישות זה.
   2. יש לבצע סקר סיכונים עדכני (לא יתקבל בדיקת פערים מסקר קודם) שבוצע במהלך שני החודשים האחרונים ליום הגשתו למשרד.
   3. המשרד ישלח צוות בחינה למשרדי המגיש כדי לעמוד על יישום הדרישות.
   4. במקרה של פערים יישלח דוח מפורט למגיש שעליו יהיה לתקן וחוזר חלילה.
   5. המשרד יעביר אישור על עמידה בפרק אבטחת המידע.
6. ביקור במשרדי המגיש בנוכחות אנשי אגף התיקשוב ונציגי האגפים הדורשים על מנת לעמוד על עמידתן של המגיש בתנאי השירות וה-SLA(כמפורט בפרק 4).
7. תתבצע עבודה מול צוות מיסור של המשרד על מנת לעמוד על עמידתו של המגיש בתנאי פרק 3 למעט סעיף 3.2 של אבטחת מידע.
8. השלב הבא הוא חיבור למערכות המשרד אולם לא יתבצע חיבור למערכות המשרד ללא הצגת לפחות אבטיפוס של פורטלי הרכש המרק"ט והנתיבים בפני נציגי המשרד.
9. לאחר הצגת האבטיפוס תתחיל עבודה מול צוות מיסור של המשרד לצורך חיבור מערכות המגיש למערכות המשרד בסביבת הטסט בלבד.
10. לאחר השלמת החיבור למערכות המשרד למעשה הוכנה התשתית לבדיקת הפורטלים (רכש, מרק"ט ונתיבים).
11. כל פורטל ייבדק בנפרד על מנת להראות לנציגי האגפים הדורשים את היתכנות פעילות הפורטל הספציפי בהפעלת תהליך שרשרת האספקה. כלומר כל פורטל ייעודי יצטרך להראות תהליך מלא החל משלב קבלת ההזמנה ועד לחשבונית כולל הצגת סטטוס חשבונית והודעות זיכוי.
12. כל תהליך יכול להתנהל בנפרד ובמקביל אך תהליך זה ינוהל בשיטה הבאה:
13. הוכחת יכולת של ממשק וקבלת ריג'קטים לתיקון.
14. לאחר ביצוע התיקון בדיקה מחודשת של הממשק ושוב ריג'קטים עד לאחר שלא יוותרו ריג'קטים לחלוטין.
15. הבדיקה תעבור לממשק הבא בתור בשרשרת האספקה של הפורטל הספציפי הנבדק.

כך למעשה עד בדיקת כל שרשרת האספקה של הפורטל הייעודי.

1. לאחר קבלת אישור מגורמי האגף הדורש שהפורטל תקין המגיש יקבל אישור על תקינות הפורטל.
2. לאחר קבלת אישור תקינות שלושת הפורטלים ניתן יהיה לעבור לשלב הבא.
3. בשלב זה תתבצע בדיקה סופית כי כלל החתימות האחרונות הנדרשות בנספחים שלא היו תקינים או היו חסרים הושלמו.
4. על המגיש להגיש את המסמכים הקשורים בערבות הבנקאית לאישור אגף הכספים של משהב"ט לבחינת התאמתם ותקינותם.
5. המשרד יאשר עמידה בדרישות סיווג קשר דיגיטלי מסחרי (קד"ם) למגיש, בכפוף להשלמת כל השלבים שלעיל בצורה מלאה ולשביעות רצון המשרד.

הבהרות ודגשים:

1. יודגש כי יתכנו שינויים ועידכונים לתהליך שלעיל והוא מפרט רק את עיקרי השלבים ולא את כלל התהליך.
2. פרק הזמן המוערך להשלמת ההליך שלעיל הינו לפחות 8 חודשים (מבוסס על נסיון העבר). יודגש כי פרק הזמן האמור הינו הערכה בלבד והוא יכול להשתנות ממקרה למקרה, למען הסר ספק יובהר כי אין באמור בערכת זמנים זו כדי לחייב את המשרד לסדר זמנים כלשהו.