נספח ענן
מכרז שירות
הרשות לתחבורה ציבורית

גרסה 1.1.0
30-06-2025

1.0 מטרת המסמך

מטרת המסמך להנחות את ספקי השירות בתהליך ההצטרפות לענן תחבורה

1.1 קהלי היעד

1.1.1 מנהלי מערכות מידע במשרד התחבורה

1.1.2 חטיבת אבטחת מידע וסייבר, משרד התחבורה

1.1.3 חטיבת תשתיות, משרד התחבורה

1.1.4 צוות CCOE, משרד התחבורה

1.1.5 מנהלים אגף טכנולוגיות דיגיטליות ומידע, משרד התחבורה

1.2 מושגים

מושג	תיאור
המשרד	משרד התחבורה, אגף טכנולוגיות דיגיטליות ומידע
ספק שירות	גוף עסקי לו התקשרות עסקית עם יחידה ארגונית במשרד התחבורה לצרכי פיתוח, הקמה תפעול ותחזוקה של מערכת מידע או שירות על פלטפורמת הענן של המשרד
צוות CCOE משרד התחבורה	צוות מקצועי במשרד המתכלל את הגישה לענן תחבורה ומהווה את הממשק בין הספק לענן תחבורה
אזור נחיתה ארגוני בענן Landing Zone	"אזור נחיתה" הוא סביבה מוגדרת עם מערך סטנדרטי של תשתית ענן מאובטחת, כללי מדיניות, שיטות עבודה מומלצות, הנחיות ושירותים מנוהלים באופן מרכזי תחת חשבון ראשי אחד .משרד התחבורה (הארגון), יוצר ואוכף מספר היבטים כנקודת בסיס עבור "היחידות הארגוניות": מדיניות אבטחה ,עבודה ברשת, קטלוג שירותים, שירותים משותפים בענן, מאגרי תבניות, ואמצעי ניטור והגנה. הארגון החשבון הראשי פועל כ"מנהל-על של הענן" הוא יכול לתת הרשאות לכל תת-גורם לפעול באופן עצמאי בהתאם למדיניות שהוגדרה, כך שמנהל-העל מחיל כללי מדיניות ומוודא שהענן ומהנדסי הפתרונות מגדירים את תצורת שירותי הענן ומשתמשים בהם בהתאם לכללים שהוגדרו מראש.

מסמך HLD (High Level Design)	מסמך הכולל דרישות עסקיות ודרישות פונקציונליות למערכת. מסמך/תרשים ארכיטקטורת הפרויקט ברמת-על, הכולל פירוט רכיבי המערכת והקשרים ביניהם, בהתאם לפתרון הענן הנבחר
ענן תחבורה	תשתית השייכת למשרד התחבורה על גבי פלטפורמה של ספקית ענן ציבורי הכולל איזור נחיתה ושירותים נוספים המשמשים להפעלת מערכות מטעם המשרד
תצורה עבודה היברידית	מערכת בענן תחבורה שלצרכי הפעלתה והרצתה נשענת על שירותים, משאבים וממשקים בחצר הארגון ו/או חצר הספק (On premises) ו/או בענן אחר
תפיסת הפעלה ספקים	נוהל מסגרת המתאר את עקרונות הפעולה, התוצרים הדרושים והתהליכים להפעלת מערכות ספק על פלטפורמת הענן של משרד התחבורה באופן שיבטיח את הפעלתן בהתאם לכללי המדיניות הממשלתית והמשרדית ועמידה ביעדי המשרד והממשלה למעבר לענן
טופס הצטרפות לענן תחבורה	איסוף דרישות על מערכות הספק שיהוו בסיס למענה ואינטגרציה עם אזור הנחיתה שיאפשרו את הפעלתה באופן יעיל מאובטח

1.3 עקרונות מנחים

1.3.1 למשרד תשתית ענן ציבורי בענן AWS בריג'ון ישראל הכולל אזור נחיתה. המערכת תפותח בסביבת הפיתוח של הספק, תותקן ותתופעל בענן בכפוף למדיניות והנחיות המשרד.

1.3.2 המערכת ו/או חלקים מהמערכת אשר תותקן ותפעל בענן תחבורה תהיה בכפוף למדיניות והנחיות המשרד והממשלה ועל פי עקרונות תפיסת ההפעלה המפורטים בנספח 1. ניתן לבצע חלוקה של מערכת לתתי-מערכות ורכיבים הנחשבים "תכולות אוטונומיות" (workloads) לצורך מענה במערכ/ות בתצורה היברידית. לאחר חלוקה זו יש לבחון מיגרציה של התכולות (תתי-מערכות ורכיבים). חלק מהמערכת שעבורה קיימות הגבלות למיגרציה לענן ימשיכו לפעול בתצורה הקיימת (retain) וחלקי המערכות יהגרו לענן בהתאם לבחינת אופן המיגרציה המתאים.

1.3.3 התשתית בענן כוללת מערך מאובטח המיועד לארח את מערכות המשרד, חיבור לתשתיות המשרד המקומיות, ניהול משתמשים, יישום מנגנוני אבטחת מידע. כמו כן הוגדרו מנגנונים לתיוג השירותים, בקרה פיננסית בסיסית (הגדרת תקציבים והתראות) מדיניות גיבויים, ניטור ולוגים לאבטחת מידע, מערכות הגנה חומת אש בתוך רשת הענן. סביבת הענן הוגדרה מתוך מטרה לשרת את המערכות המתוכננות להגר ו/או לפעול בענן.

1.3.4 הספק הזוכה יידרש לתהליך הצטרפות לענן תחבורה בו יכיר את הדרישות, הנחיות ועקרונות ההפעלה. כחלק מהתהליך יידרש הספק להגיש למשרד טופס הצטרפות לענן תחבורה, לאפיין ולהקים את המערכת באזור ייעודי שיוקם עבורו על ידי המשרד ולבצע אינטגרציה של המערכות ומרכיביה עם אזור הנחיתה של המשרד בכדי לאפשר תפעול יעיל ומאובטח.

1.3.5 המדיניות הממשלתית לעבודה בענן מחייבת עבודה באזור נחיתה. אזור הנחיתה, המערכת ושירותי התשתית בענן יוקמו ויופעלו באזורי הספק הענן (region) בישראל או לפי הנחיה אחרת של המשרד.

1.3.6 ארכיטקטורת המערכת תעוצב ותבנה בגישה Cloud Native שתבטיח ניצול טכנולוגיות ויכולות ענן באופן מיטבי ועדכניות טכנולוגית שתשמר את חיי המערכת מבלי להשפיע על אספקת השירות או אימוץ ארכיטקטורות מערכת מותאמות לענן.

1.3.7 חשבונות ורשתות תקשורת (Networking): לספק יוקצה אזור ייעודי בענן הכולל חשבונות ורשתות תקשורת VPC שיפרסו על ידי צוות הענן המשרד. מבנה החשבונות והרשתות, תעבורה יוצאת Egress ותעבורה נכנסת Ingress לגישה של משתמשים מרשת האינטרנט תהיה בהתאם לארכיטקטורה ומדיניות המשרד .

1.3.8 ארכיטקטורת המערכת על גבי תשתיות הענן תתמוך ברכיבים בתפיסת PaaS/SaaS ושירותים מנוהלים, לדוגמה Function as a Service , Database as a Service וכדומה. פתרון מבוסס IaaS, יוקם במקרים בהם לא קיימת חלופת PaaS/SaaS או בהתאם לשיקולים אחרים כגון אבטחת מידע, רגולציה, יעילות ובכפוף לאישור המשרד.

1.3.9 למשרד רשימה של מוצרים ושירותים צד ג' המחליפים שירותי ענן cloud native, לדוגמה: שירות חומת אש Cloud guard של חברת Check point, שירות הלבנת קבצים Opswat ואחרים. הספק יחויב לעשות שימוש בשירותים אילו. מקרים חריגים ידונו בוועדת הענן של המשרד. בנוסף, במסגרת מכרז רובד 5 של נימבוס תתאפשר צריכה של שירותים כאלו מתוך קטלוג השירותים (שוק דיגיטלי) הממשלתי של ספקיות הענן. רכש שירותי צד ג' בשוק הדיגיטלי: ככלל, ירכשו השירותים הזמינים בשוק הדיגיטלי של ספקי הענן בהתאם להודעת מכרז מרכזי, " אספקת שירותי ענן ציבורי של AWS ו-Google למשרדי הממשלה", מס' 16.12.2 והודעת מכרז מרכזי, "רכש ומימוש שירותי צד ג' בענן הציבורי של AWS ו- Google", מס' 16.12.3. בהתאם להודעת מכרז מרכזי, "פרויקט נימבוס – הנחיות כלליות בנוגע לרכש שירותי ענן ציבורי", מס' 16.12.1 ולהודעת מכרז מרכזי, "רכש ומימוש שירותי צד ג' בענן הציבורי של AWS ו- Google", מס' 16.12.3, מזמין רשאי לערוך הליך רכש עצמאי עבור שירות ענן מסוים.

1.3.10 הספק יידרש להציע פתרון התומך בתשתית הענן ולתאר פתרון זה באמצעות תרשימי ארכיטקטורה הכוללים את כל הרכיבים ואופן התממשקות ביניהם. תיאור הפתרון נדרש לפרט את תצורת התשתית, השירות/ים והרכיבים שנדרשים ליישום, וזאת תוך הבטחה לעמידה בזמינות, שרידות, ובהיקף הגידול העתידי בהתאם לדרישות המערכת. התרשימים יוכנו בכלים תקניים, לדוגמת Draw.io ויותאמו לספק הענן שנבחר. תיאור הפרויקט יכלול לכל הפחות תיאור תשתית, תיאור רכיבים אפליקטיביים עיקריים, תיאור פתרון אבטחת מידע, תיאור פתרון לזמינות ושרידות המערכת וכן תיאור כל הממשקים פנימיים (ספקית הענן) וחיצוניים (מערכות בענן וחצר המשרד). לשיקול דעתו של הספק להוסיף תיאורים נוספים המשפרים את הבנת הפתרון המוצע.

1.3.11 הפתרון המוצע יידרש להתייחס לתצורה המתאימה לעבודה בענן ולשם כך יש לפרט את כל הרכיבים והמשאבים הנדרשים לפתרון כולל שירותים, כלים, רישוי, אחסון עלות וכמויות. יש להתייחס לתקופת ההרצה / הקמה, הפעלה שוטפת של המערכת, גמישות תפעולית ויכולת גידול בהתאם לצורך בהמשך ההפעלה של המערכת (Scalability). תחשיב העלויות והכמויות יכלול את כל הסביבות הנדרשות לפרויקט לרבות סביבות פיתוח, בדיקות ויצור כפי שמפורט מטה בסעיף 1.3.13

1.3.11.1 הספק יידרש להכין ולהציג את מסמך HLD (High Level Design) לסקר המשרד כחלק מתהליך ההצטרפות אשר יכלול את הפרטים המפורטים לעיל

1.3.12 הפתרון יידרש לאישור המשרד

1.3.13 המדיניות הממשלתית מחייבת הפרדת סביבות Prod/ Non Prod. עבור כל מערכת ייצור שתועבר לענן יש לתכנן את, סביבת הפיתוח וסביבת הבדיקות (NonProd), וכל סביבה אחרת משלימה למערכת הייצור (PROD). עבור סביבות NonProd יש לפעול על פי ה- Best Practices להדלקה וכיבוי הסביבה באופן אוטומטי וידני וכן אפשרות לשכפול המערכות. על כן יש לייצר Pipelines בקוד (IAC) כדי לאפשר הקמת הפרויקט בכל סביבה. כחלק מהפרויקט המציע יקים סביבת פיתוח, סביבת בדיקות וכן יבצע את ההגירה לסביבת הענן המשרדי. בדיקות המסירה, קבלה, ביצועים ואבטחת המידע יתבצעו בסביבת הבדיקות, בטרם עלייה לאוויר או כל סביבה אחרת עליה יורה המשרד.

1.3.14 לאחר סיום מוצלח של הבדיקות שפורטו לעיל ואישור תקינות התוצרים על ידי המשרד, המציע יתקין את התוצרים בסביבת הייצור בהתאם לתוכנית העבודה שתסוכם בפרויקט.

1.3.15 פיתוח/קידוד: כל פעילות הקשורה לפיתוח משלב האפיון ואילך נדרש להיות מנוהל בהתאם להנחיית המשרד כולל קוד המקור שיפותח ע"י, ויחולו ההנחיות הבאות:

- תוצרי פיתוח יפותחו בכלי לניהול גרסאות וכל גרסאות הקוד יועברו למשרד
- כל קוד שנכתב ילווה בהגדרה וביצוע של Unit Test.
- ה- Unit Test יכסו פונקציונליות בהיקף כיסוי מקיף
- ניהול כל פעילות הפיתוח תחת Source Control .
- הקוד יעבור בדיקה של איש תוכנה של הספק, שאינו המפתח של אותו קוד.
- תהליך הפצת גרסאות מערכת יבוצע בתיאום מלא ואישור צוות DevOps במשרד.
- על הספק הזוכה לבצע בדיקות אבטחת קוד על הקוד שיפותח תוך התייחסות לסיכוני אבטחת מידע אפליקטיבי בהתאם להנחיות חטיבת אבטחת מידע של המשרד
- הפיתוח יבוצע בהתאם לנוהל פיתוח מאובטח (ראה נספח הנחיות אבטחת מידע)
- הספק יוודא קיום של תיעוד המערכת כולל: חומרים הטכניים המעודכנים, הנחיות למפעיל המערכת לרבות התקנה, הפעלה, כיבוי ושדרוג המערכת, הנחיות למשתמש, הנחיות לזיהוי וטיפול בבעיות. פיתוח המערכת ילווה בכתיבה של הערות בקוד באופן נרחב ומאפשר הבנה של הקוד ע״י אנשי פיתוח/ארכיטקטים של המשרד

1.3.16 שכבת שירותים, קישוריות ואינטגרציה : על הספק לפרט את כלל ממשקי המערכת בסביבת הענן. כל ממשק יהיה חייב באישור המשרד ויאופיין בהתאם לתקן ממשקים של המשרד. התבססות על

פתרון שדרת המידע הממשלתית לקישוריות שירותים עם משרד ממשלה אחרים או גופים מסחריים כמו בנקים או לשירותים הפועלים בחוות השרתים המשרדית.

1.3.17 שימוש בשירות אחסון ענני בהתאם למדיניות הגישה והארכוב (S3)

1.3.18 קישוריות אתר ספק לסביבת הענן של המשרד: הספק יידרש לקישוריות מאובטחת באמצעות IPVPN או חיבור ברכישת קו AWS Direct Connect הצפנה והגנה של התווך יהיו באמצעות מוצרים וכלים שיאושרו על ידי המשרד.

1.3.19 גיבוי ושחזור: תהליכי הגיבוי והשחזור יהיו באחריות הספק בהתאם לדרישות העסקיות ומדיניות הגיבוי והשחזור של המשרד. מערכות הגיבוי והשחזור יאושרו על ידי המשרד. על הספק לבצע בדיקות גיבוי ושיחזור בהתאם למדיניות המשרד וכן לנהל יומן הפעלות.

1.3.20 לוגים, התרעות וניטור: הספק יידרש לבצע ניטור לשירותים ולמערכות בתחום אחריותו במערכות ניטור שיאושרו על ידי המשרד. איסוף הלוגים והניטור יהיו במספר רבדים: אבטחת מידע, רשת והמערכת (אפליקציה). כחלק מהפעלת ה- WL באזור הנחיתה של המשרד הוגדר תהליך מרכזי לאיסוף לוגים מכלל המערכות והשירותים לצורך בקרה, ניטור והתראה ואופיין מודל חלוקת אחריות בין הספק למשרד לטיפול באירועים ותקלות. לוגים ישמרו למשך תקופה המצוינת במסמך תפיסת ההפעלה.

1.3.21 זמינות, שרידות והמשכיות עסקית: המפעיל נדרש לזמינות ברמה החודשית, כולל השבתות יזומות, של המערכת. על הספק להציג שיטות ,תהליכים ארגוניים, ארכיטקטורה כלים ואמצעים להתאוששות מנפילות ותקלות שיאפשרו עמידה בדרישה זו. מדדי RTO , RPO יקבעו על ידי הגוף העסקי מטעם המשרד.

1.3.22 משתמשים והרשאות: גישה של הספק לענן תחבורה לצרכי פיתוח, תפעול ותחזוקה של המערכות יהיו בהתאם להנחיות המפורטות במסמך ההפעלה ספקים. הקמה ושיוך משתמשים יתבצע על ידי צוותי התפעול של המשרד.

1.3.23 תיוג (Tagging) תיוג המערכות באחריות הספק ובהתאם למדיניות המשרד.

1.3.24 ניהול הקוד ואוטומציה

1.3.24.1 ניהול תשתית כקוד Iac: הספק יקים, יפרוס וינהל את תשתית הענן באמצעות קוד Iac (Infrastructure as a code) ובכלים לניהול תשתית כקוד. על הקוד להיות כתוב בכלי גנרי כמו Terraform חריגה או בקשה לבניית הקוד בכלי שונה תיעשה באישור הגורמים המוסמכים במשרד).

1.3.24.2 אוטומציה CI/CD: תהליך הפיתוח, האינטגרציה וההפצה של גרסאות התוכנה יהיו בכלי אוטומציה ויתבססו על מתודולוגיית CI/CD. על הספק להציג מתודולוגיית CI/CD עבור המערכת הכוללת הקמה, הגנה ותחזוקה של תהליכי PIPELINE בין סביבות נמוכות ובין TEST לסביבת הייצור. יודגש כי על הספק להפעיל את אותם תהליכים בכל הסביבות כולל סביבות נמוכות וסביבות פיתוח. פיתוח IAC יתבסס על אותם הכללים כמו פיתוח האפליקציה המפורטים בסעיף 1.3.15

1.3.25 הספק יפתח את רכיבי התוכנה כשירותים עצמאיים שיאפשרו גדילה לרוחב בהתאם לעומס של שירותים מרכזים, ולא כיחידה מונוליטית אחת.
למשל, container ו serverless על Docker.

1.3.26

1.3.27 כלכלת ענן

1.3.27.1 הערכת עלויות תתבצע לאחר החלטה על ארכיטקטורת המערכת ותכנון שלבי הפרויקט. יש להעריך עלויות עבור כל שלב בהטמעת המערכת החל משלב בדיקות היתכנות, פיתוח, בדיקות, ייצור. על מנת להעריך את העלויות ניתן להיעזר במחשבוני עלויות המסופקים על ידי ספקי הענן . בעת הערכת עלויות הפרויקט יש לקחת בחשבון עלויות נוספות, שאינן כחלק ממשאבי הענן הנרכשים, לצורך יצירת הערכת עלויות מדויקת ככל הניתן, כגון עלויות אזור הנחיתה, תעבורת רשת, עלויות כלי ניטור, עלויות הרישוי, כלי בקרה ואבטחת מידע .

1.3.27.2 יש להשתמש בסימולטורים/מחשבונים של ספקיות הענן לקבלת הערכת עלויות (מחשבון AWS). יש להציג 3 תחשיבים: Pay as you go, 1-year commitment no upfront, 3-yaers commitment – no upfront. המשרד יפעיל מנגנון הנחות באופן עצמאי על בסיס הערכות אשר יועברו עליו.

1.3.28 על הספק לבצע הערכת עלויות עבור כל אחת מסביבות העבודה ולצרפו כדוח כחלק מתהליך ההצטרפות

1.3.29 אישור מנהל היחידה עסקית מטעם המשרד את עלות המשאבים והצריכה השוטפת

1.3.30 ארכיטקטורת המערכת תבנה באופן שתמקסם את הערך מבחינת ביצועי המערכת והעלות השוטפת ובהתאם לשיטות העבודה המומלצות.

1.3.31 הגדרת מנגנון מעקב אחר אופן וקצב ניצול התקציב והגדרת התראות על ניצול התקציב (ניצול של 25%, 50%, 75%, 90%, וכן הלאה).

1.3.32 טיפול בתקלות בשירותי הענן

ענן תחבורה פועל לפי כללי מכרז נימבוס בהתאם לחוזה תמיכה הנכלל בו, ומאפשר לבעלי הרשאה לפתוח קריאות ב console הענן, במידה וצוות הספק נתקל בתקלה בשירותי הענן הציבורי, יכול מורשה מטעם הספק לפתוח קריאה להתנהל מול התמיכה של הספקית בצורה עצמאית. במידה ויהיה צורך לשלב מענה מצוות המשרד, יפנה מנהל הענן מטעם הספק או מנהל הפרויקט במשרד לצוות המשרד בדוא"ל והצוות ייתן מענה.

1.3.33 הספק יכיר ויעמוד בהנחיות אבטחת המידע והגנת הסייבר של המשרד, הנחיות מערך הדיגיטל הלאומי (המפורסמות באתר מערך הדיגיטל), יה"ב ושיטות העבודה המומלצות.

1.4 נספחים

1.4.1 מסמכי ארכיטקטורה של אזור הנחיתה בענן AWS , תפיסת הפעלה וטופס הצטרפות יועברו לספק לאחר אישור הזכייה

1.4.2 נספח אבטחת מידע וסייבר מכרז - יסופק על ידי מנהל אבטחת המידע המלווה את הפרויקט

1.4.3 רכש שירותי צד ג' בשוק הדיגיטלי: ככלל, ירכשו את השירותים הזמינים בשוק הדיגיטלי של ספקי הענן בהתאם להודעת מכרז מרכזי, "אספקת שירותי ענן ציבורי של AWS ו-Google למשרדי הממשלה", מס' 16.12.2 והודעת מכרז מרכזי, "רכש ומימוש שירותי צד ג' בענן הציבורי של AWS ו- Google", מס' 16.12.3. בהתאם להודעת מכרז מרכזי, "פרויקט נימבוס – הנחיות כלליות בנוגע לרכש שירותי ענן ציבורי", מס' 16.12.1 ולהודעת מכרז מרכזי, "רכש ומימוש שירותי צד ג' בענן הציבורי של AWS ו- Google", מס' 16.12.3, מזמין רשאי לערוך הליך רכש עצמאי עבור שירות ענן מסוים. במקרה זה, על המזמין לפעול בהתאם לכללים המפורטים בהודעה זו.