# אסטרטגיית הענן הממשלתית

נובמבר 2022

# אסטרטגיית הענן הממשלתית

נובמבר 2022

משרד ראש הממשלה
אגף התקציבים
החשב הכללי
Accountant General
סייבר ישראל
מערך הסייבר הלאומי
מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

**הובלת צוות האסטרטגיה:** רחל רן, מערך הדיגיטל הלאומי

**חברי צוות האסטרטגיה ושותפים לכתיבת המסמך:**

מערך הדיגיטל הלאומי: עו"ד יערה בן שחר-תיק, ניר בר יוסף, קרן בר לב, עו"ד ג'יין ווגל כוחי, טל חכים, ענת קוסיאק, רחל רן, אלון תקוע

משרד האוצר, מנהל הרכש הממשלתי: שאול גבעולי, עו"ד צביאל גנץ, עמרי נצר

משרד האוצר, אגף התקציבים: אריאל הבר

משרד ראש הממשלה: עדו קמחי-פלדהורן

מערך הסייבר הלאומי: אורן בושמיץ, טלי שמר

**תודות לשותפים להובלת פרויקט נימבוס והתפיסה האסטרטגית של הענן בממשלה:**

יגאל אונא

גל אמיר

שחר ברכה

רועי דרור

מוריה זיסוביץ'

אייל טולדו

שירה לב-עמי

גבי פורטנוי

רפאל פרנקו

אביתר פרץ

אלי קורח

אבישי קראוס

טל שחם

יוגב שמני

**ייעוץ טכנולוגי:** חברת KPMG סומך חייקין

## תוכן עניינים


תקציר מנהלים ........ 6

1 | אסטרטגיית הענן - מטרה ותחולה ........ 9

2 | מחשוב ענן בממשלה ........ 10

3 | חזון הענן הממשלתי ומרחב ההזדמנויות ........ 16

4 | אסטרטגיית הענן הממשלתית – מטרות ויעדים ........ 22

5 | תפיסת הפעלה לענן בממשלה ........ 24

6 | ניהול סיכונים ........ 32

7 | מדדי הצלחה למעבר הממשלה לענן ........ 39

8 | יוזמות אסטרטגיות וצעדים להמשך ........ 43

נספח א | מילון מונחים ........ 45

נספח ב | עקרונות לסיווג מידע במעבר לענן ........ 50

# תקציר מנהלים

האצת פלטפורמות הענן בעשור האחרון הובילה לשינוי פרדיגמה באספקת שירותים טכנולוגיים, כאשר יותר ויותר חברות מעבירות את המוצרים והשירותים המוצעים על ידיהן לתשתיות ענן. במסגרת מגמה זו, היצע המוצרים והטכנולוגיות הזמינים להתקנה ולמימוש בתשתיות ארגוניות מקומיות (להלן: "On Premises") הולך ומצטמצם, והיצע החדשנות ממוקד בענן הציבורי. מנגד, השימוש בתשתיות ענן ציבורי מייצר מורכבות משפטית ומשילותית ומעלה שאלות לגבי ריבונות המידע, הרגולציה וההסדרים המשפטיים החלים עליו.

במצב הדברים שקדם לפרויקט "נימבוס" נדרשה הממשלה להכריע בין שתי חלופות לא מיטביות: להמשיך ולהשקיע בתשתיות On Premises וכתוצאה מכך לוותר על פוטנציאל חדשנות והתקדמות טכנולוגית, או להרחיב את השימוש בשירותי ענן ציבורי מחוץ לתחומי ישראל, תוך סיכון לריבונות ולהגנה על נכסיה הדיגיטליים של הממשלה. על רקע זה קם "נימבוס", פרויקט דגל רב-שנתי רחב היקף, המקודם על ידי מינהל הרכש הממשלתי ומערך הדיגיטל הלאומי, בשיתוף עם מערך הסייבר הלאומי, הממונה על התקציבים במשרד האוצר ואגף ממשל וחברה במשרד ראש הממשלה, במטרה לתת מענה מקיף לנושא אספקת שירותי ענן עבור ממשלת ישראל. ייחודו של הפרויקט בכך, שאל מול חלופות שנראו כדרך ללא מוצא הוא סלל את הדרך להקמת ענן ציבורי בשטח ישראל ופתח את הדלת לענן עבור הממשלה.

מעבר הממשלה לענן אינו רק מהפכה טכנולוגית, אלא גם מהפכה ארגונית ועסקית, המשנה את תפקידה של הטכנולוגיה בארגון, מציבה במרכז את צורכי המשתמשים ואת המיקוד ביצירת ערך, ומייצרת מרחב הזדמנויות חדש, לרבות השפעה כלכלית ומשקית נרחבת.

מתוך הבנה זו, ממשלת ישראל גיבשה חזון עתידי לאימוץ שירותי ענן ציבורי מתקדמים במטרה לשפר את השירות לציבור, להגביר את אפקטיביות המדיניות הממשלתית, להאיץ תהליכי חדשנות ולחזק את יכולותיו המקצועיות של המגזר הציבורי, תוך קידום התייעלות כלכלית, מקסום הגמישות הטכנולוגית ושמירה על הגנה בסייבר ואבטחת מידע. חזון הענן הממשלתי רואה בפרויקט "נימבוס" זרז לשינוי תהליכי עומק, המשפיעים על עבודת הממשלה בכל רבדיה, באמצעות היכולת לממש פתרונות טכנולוגיים הנותנים מענה לקצב התדיר של השינויים בצרכים, באופן צריכת השירותים ובסדרי העדיפויות. מימוש מלא של החזון יוביל ל"אפקט אדווה", שגליו ישפיעו על כל היבטיה של פעילות הממשלה, המגזר הציבורי הרחב והמשק כולו.

מתוך מרחב ההזדמנויות שמייצר המעבר לענן, ולאור ההבנה כי מהלך זה מלווה בתהליכי שינוי מורכבים, הדורשים ריכוז מאמצים ומיקוד מקצועי, אסטרטגיית הענן הממשלתית מתמקדת בכמה מטרות ליבה לענן בשנים הקרובות:

1. שיפור השירותים והמוצרים הדיגיטליים לציבור - אזרחים ועסקים.
2. ביצוע קפיצת מדרגה ביכולותיה הטכנולוגיות של הממשלה.
3. שיפור האפקטיביות וייעול ההוצאה הממשלתית בתחום הטכנולוגיה.
4. חיזוק היכולות המקצועיות של הממשלה.
5. הבטחת המשילות, הריבונות וההגנה בסייבר על התשתיות הטכנולוגיות והמידע הממשלתי בענן.

המיקוד מאפשר גיבוש יעדים מדידים להתקדמות ובשלות הענן בממשלה, ומניח את היסודות להרחבת הפעילות למטרות ולמעגלי השפעה נוספים בעתיד, בדגש על פוטנציאל ההשפעה של פרויקט "נימבוס" על המשק והסקטור העסקי.

על מנת לממש את מטרות הענן ואת יעדיו גיבשה הממשלה תפיסת הפעלה הוליסטית, הכוללת עקרונות אופרטיביים וכיווני פעולה בכל אחד מהיבטי השינוי שמחולל הענן. במסגרת זו מגדירה אסטרטגיית הענן עקרונות פעולה בכמה צירים מרכזיים:

- **מדיניות:** הקמת מרכז מצוינות מקצועי לענן – CcoE (Cloud Center of Excellence), המהווה גוף הניהול והמדיניות לתחום הענן. ה-CCoE הוא גוף על-ארגוני, המורכב מכלל הגורמים הממשלתיים השותפים למהלך ופועל בתפיסה מטריציונית באמצעות צוותים חוצי-תחומים. ל-CCoE כמה תפקידי מפתח: התוויית אסטרטגיה ומדיניות ליישום הענן בממשלה, סטנדרטיזציה ומשילות IT, הנחיה מקצועית, ארכיטקטורה, ניהול סיכונים וסייבר, מידע ורגולציה, מדיניות רכש ופיננסים בענן (FinOps), תכנון מרכזי לפיתוח שירותי IT משותפים וכן מינוף וחשיפה של תחום הענן בממשלה.
- **טכנולוגיה:** העיקרון המנחה את הממשלה הוא ענן תחילה (Cloud First), המתעדף את הבחירה בתשתיות ענן כברירת מחדל. לצד עיקרון זה תקדם הממשלה הגירה (מיגרציה) לענן של מערכות קיימות ויישום עקרון "אזור נחיתה" (Landing Zone), בדגש על ניהול מרכזי, תוך שמירה על עצמאות תפעולית. תפיסה זו מלווה בעקרונות משלימים של אוטומציה בתהליכים ומשימות תשתית וכן שיתוף קוד והפצת פתרונות ממשלתיים.
- **התנהלות פיננסית:** עקרונות הפעולה כוללים ליווי של תהליכי הבחינה הפיננסית של הפרויקטים המקודמים, שילוב של תהליכי התכנון הפיננסי בעבודה הארגונית הטכנית, ביצוע של ניתוחי עומק של השימושים הארגוניים בענן והתאמות ואופטימיזציה בשירותים.
- **ניהול השינוי הארגוני:** ניהול השינוי יתבצע תוך מיקוד ביצירת ערך עבור משרדי הממשלה, יצירת תהליך עבודה משתף, שיתוף ידע מקצועי ושקיפות, תוך הקניית מיומנויות ייעודיות והתאמת המבנה הארגוני וההון האנושי הממשלתי לעבודה בענן.
- **עקרונות להגנת סייבר בענן ודרכי מימוש:** ניהול סיכונים והערכת סיכוני סייבר, בקרות ואמצעי הגנה, סיווג המידע והמערכות, קווים מנחים וסטנדרטיזציה עבור משילות ותפעול של מערכות בענן, אבטחה של תהליכי פיתוח, ניהול זהויות ובקרת גישה ועוד, כמפורט בפרק 6.2 במסמך זה.

רוחב היריעה ומורכבותו של נושא הענן, ובפרט מעבר הממשלה לענן ציבורי, מחייבים תפיסת הפעלה, המבוססת על שיתוף הפעולה המקצועי עם כלל בעלי העניין והשותפים, המהווים חלק אינטגרלי במהלך: בראש ובראשונה, משרדי הממשלה ויחידות הסמך, שהינם מובילי מהפכת הענן ומימושה באמצעות אגפי טכנולוגיות דיגיטליות ומידע, מנוע ההצלחה של אסטרטגיית הענן הממשלתית. לצד המשרדים, המעבר לענן מושתת על הובלה מקצועית של מערך הדיגיטל הלאומי ומינהל הרכש הממשלתי, בשיתוף הדוק עם גורמי המטה בממשלה, ובהם משרד ראש הממשלה, הממונה על התקציבים במשרד האוצר, החשב הכללי ומערך הסייבר הלאומי. יצירת שיתוף פעולה מקצועי מלא ורתימת כלל השותפים לתהליך הן תנאים הכרחיים להצלחת המהלך. על מנת לוודא כי הממשלה פועלת בערוצים המקדמים את המטרות והיעדים המוגדרים באסטרטגיית הענן יוקם מערך מדידה רב-תחומי, אשר ילווה את הגורמים השותפים בהגדרת מדדי ההצלחה, בביצוע המדידה ובניתוח הנתונים לטובת קבלת החלטות מושכלות ודיוק כיווני הפעולה.

לצד היתרונות הברורים והחשובים של המעבר לענן, על הממשלה להתייחס למרחב סיכונים חדש, הכולל סיכוני סייבר, סיכוני IT, משילות המידע, סיכונים פיננסיים ועוד. סיכונים אלו מחייבים איזון מורכב בין מתן מרחב פעולה וניצול אופטימלי של יכולות הענן והגמישות שהוא מייצר לבין הצורך להגן על נכסיה הדיגיטליים של הממשלה. בהקשר זה, תנאי מכרז "נימבוס" והקמת תשתיות ענן ציבורי בשטח מדינת ישראל צפויים לתת מענה לשאלת ריבונות המידע, כמו גם להבטיח את המשכיות האספקה

של שירותי הממשלה לאזרחים גם במקרי קיצון. לצד המענה המכרזי, מימוש אסטרטגיית הענן הממשלתית יכלול מדיניות ניהול סיכונים מפורטת וסדורה לשימוש משרדי הממשלה.

בעשור האחרון השקיעה הממשלה משאבים ומאמצים רבים בטרנספורמציה דיגיטלית ובחיזוק יכולותיה הטכנולוגיות, וחלה התקדמות רבה בתחום. עם זאת, בחלק מההיבטים הממשלה עדיין מצויה בפער ביחס לשוק הפרטי. מבחינה זו, מעבר הממשלה לענן מהווה שינוי טקטוני בדפוסים ובמנגנוני הפעולה וביכולתה לרתום טכנולוגיה לטובת שיפור השירות לציבור וחיזוק האפקטיביות, תוך ביצוע "חריש עמוק" ביכולות ובמערכות הקיימות. אסטרטגיית הענן הממשלתית, המתוארת במסמך זה, מניחה לפתחה של הממשלה הזדמנות לצמצם את הפער הקיים ולחזק את החיבור בין הטכנולוגיה לצרכים המקצועיים והעסקיים ולבצע את קפיצת המדרגה הנדרשת כדי לממש את יעדיה.

# 1 | אסטרטגיית הענן - מטרה ותחולה

באוגוסט 2021, עם התקדמות פרויקט "נימבוס", לאחר השלמת השלבים המכרזיים הראשונים ולקראת מימושו, קיבלה הממשלה את החלטה מס' 231 בדבר קידום המעבר הממשלתי לענן ציבורי. במסגרת ההחלטה נקבע, כי יוקם צוות בראשות מערך הדיגיטל הלאומי ובהשתתפות משרד ראש הממשלה, אגף התקציבים במשרד האוצר, מינהל הרכש הממשלתי ומערך הסייבר הלאומי ("צוות אסטרטגיה"), אשר יגבש אסטרטגיה ממשלתית ארוכת טווח למעבר לענן הציבורי.  מסמך זה גובש מכוח החלטת הממשלה, ומפרט את עיקרי האסטרטגיה הממשלתית למעבר הממשלה לענן במסגרת פרויקט "נימבוס".

אסטרטגיית הענן נועדה לשמש כמצפן וכמסגרת מארגנת לכלל הפעילות הממשלתית בתחום הענן, כאשר ממנה תיגזר במעלה הדרך מדיניות מפורטת בכל אחד מתחומי האסטרטגיה, ובכלל זה מדיניות ההגירה לענן, התוויית מדיניות מרכזית לאופן המימוש של מערכות המחשוב של המשרדים ויחידות הסמך בענן, קביעת אמות מידה לסיווג מידע ומערכות כחלק מתהליך המעבר לענן, איתור צרכים רוחביים והתאמתם לפתרונות הענן הזמינים, יצירת תהליכי הדרכה, הכשרה והתמקצעות בקרב הממשלה בעבודה על תשתית הענן, יצירת מתווה להתאמת ההון האנושי וכן קביעת מדיניות הגנה, אבטחה ובקרה בסייבר בענן ציבורי.

האסטרטגיה המפורטת במסמך זה היא תוצר של תהליך חשיבה וגיבוש, שנעשה בשותפות בין-משרדית עם הגורמים החברים בצוות האסטרטגיה ובסיוע חברת הייעוץ KPMG, אשר מלווה את הקמת ה-CCoE במסגרת רובד 2 של מכרז "נימבוס" (ראו סעיף 2.3 למסמך זה). התהליך כלל למידה מהנעשה בעולם בכלל ובממשלות ובתאגידי ענק בפרט, גיבוש חזון ומטרות למהלך, התייעצות עם מומחים מקצועיים וסדנאות עבודה. בהמשך יתקיימו מפגשי שיתוף של בעלי עניין מרכזיים, ובראשם מנהלי אגפי טד"מ בממשלה (טכנולוגיות דיגיטליות ומידע), דיוני הכרעה וקבלת החלטות בצומתי הכרעה משמעותיים. התוצר הסופי המונח לפניכם מתאר את חזון הענן בממשלה, את מטרותיו ויעדיו ואת תפיסת ההפעלה למימושו.

# 2 | מחשוב ענן בממשלה

האצת פלטפורמות הענן בעשור האחרון הובילה לשינוי פרדיגמה באספקת שירותים טכנולוגיים, כאשר יותר ויותר חברות מעבירות את המוצרים והשירותים המוצעים על ידיהן לתשתיות ענן, בעיקר במודל של "תוכנה כשירות" (Software as a Service, להלן: "SaaS" - ראו בהמשך פרק זה). במסגרת מגמה זו, היצע המוצרים והטכנולוגיות הזמינים להתקנה ומימוש בתשתיות ארגוניות מקומיות (להלן: "On Premises") הולך ומצטמצם, כך שהיצע החדשנות ממוקד בענן הציבורי. מנגד, השימוש בתשתיות ענן ציבורי מייצר מורכבות משפטית ומשילותית ומעלה שאלות לגבי ריבונות המידע, הרגולציה וההסדרים המשפטיים החלים עליו, בפרט כאשר התשתית הפיזית ממוקמת מחוץ לגבולות מדינת ישראל. במצב הדברים שקדם לפרויקט "נימבוס" לא הוצעו שירותי ענן ציבורי על גבי תשתית הממוקמת בגבולות מדינת ישראל, והממשלה נדרשה להכריע בין שתי חלופות לא מיטביות: להמשיך ולהשקיע בתשתיות On Premises וכתוצאה מכך לוותר על פוטנציאל חדשנות והתקדמות טכנולוגית, או להרחיב את השימוש בשירותי ענן ציבורי, תוך סיכון מסוים לריבונות ולהגנה על נכסיה הדיגיטליים של הממשלה. על רקע זה קם פרויקט "נימבוס", אשר למול חלופות שנראו כדרך ללא מוצא אפשר הקמה של ענן ציבורי בשטח ישראל ופתח את הדלת לענן עבור הממשלה.

מעבר הממשלה לענן אינו רק מהפכה טכנולוגית, אלא גם ארגונית - זמינותם של פתרונות התוכנה החדשניים והמתקדמים בעולם, לצד הפחתת התשומות המושקעות בניהול התשתיות ותחזוקתן, משנים את תפקידה של הטכנולוגיה בארגון ושמים במרכז את צורכי המשתמשים ואת המיקוד בערך העסקי עבור הארגון. מטרת פרק זה היא לשרטט את הציר המחבר בין התפתחות פלטפורמות הענן לבין המצב הקיים בממשלה ביחס למימוש טכנולוגיה ודיגיטל, למפות את האתגרים המשפיעים על אימוץ טכנולוגיות ענן ולהניח את היסודות להיכרות עם פרויקט "נימבוס" והשינוי שהוא צפוי לייצר.

## 2.1 מחשוב ענן - רקע

מחשוב ענן הוא אחת המגמות הדומיננטיות ביותר בעולמות הטכנולוגיה בשני העשורים האחרונים. טכנולוגיות מחשוב הענן מאפשרות שיתופי פעולה בין צוותים בכל העולם ומעבר לתפיסת עבודה של עבודה-מכל-מקום, שבעזרתם ארגונים יכולים להשתחרר מהצורך לנהל ולתחזק את חוות השרתים והחומרה שברשותם, ומנהלי מערכות המידע יכולים להתמקד בפעולות ליבה – פיתוח יישומים, שיפור התוצאות העסקיות של הארגון ושיפור השירות לאזרחים, זאת תוך בקרה שוטפת אחר ההוצאות של תחום תשתיות המידע.

את הגידול באימוץ פתרונות ענן ניתן לייחס ל-2 סיבות עיקריות:

- **ניהול משאבים:** הרעיונות שמאחורי טכנולוגיות הענן קיימים כבר משנות ה-50' כמענה לעלויות הגבוהות שנדרשו לקנייה וניהול של מחשבים פרטיים. בשנות ה-70' הנחילה חברת "IBM"את רעיון השימוש במחשבים וירטואליים - פתרונות תוכנה המאפשרים יצירת כמה מכונות וירטואליות, המאוחסנות ומתופעלות תחת אותו שרת מארח. כיום השימוש בענן הוא בתצורת "as-a-Service" (ראו בהמשך פרק זה).
- **שיתוף משאבים (Collaboration):** מאז ומעולם אחד האתגרים הטכנולוגיים הגדולים שעמדו בפני ארגונים היה כיצד לשתף משאבים (מחשבים, שרתים, מידע וכו') בין כל העובדים בארגון. לדוגמה, העבודה עם Virtual Private

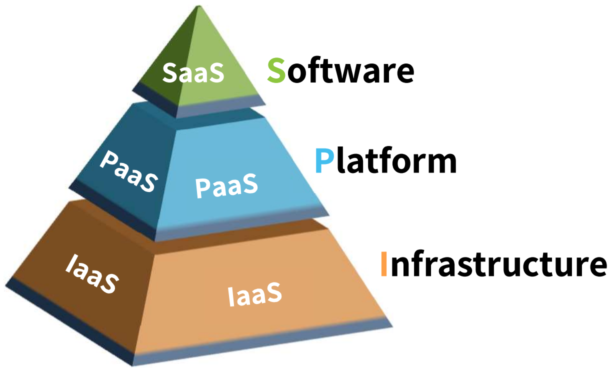
(VPN)Networks הייתה פריצת דרך בשיתוף המשאבים בין עובדים באזורים שונים בעולם. פתרונות של שיתוף כלים ומשאבים בעזרת אפליקציות פשוטות לשימוש הם אחת ההבטחות של פתרונות הענן. המעבר של מיליוני אנשים לעבודה מהבית בעקבות פרוץ הקורונה ב-2020 אפשר לארגונים רבים לעבור לשימוש בתשתיות הענן כבסיס לשיתוף משאבים שונים, ובכך לאפשר לעובדים שלהם עבודה ללא שינוי.

## מהו ענן?

הענן הינו הסטנדרט החדש לצריכה של מידע ושירותים. צריכת משאבי מחשוב (כגון אחסון ושרתים) נעשית על פי דרישה, ובכך מאפשרת לארגונים המאמצים את הסטנדרט הזה לעבור לתהליכי עבודה מדרגיים, גמישים וכתוצאה מכך, קיצור זמני הפיתוח של שירותים דיגיטליים חדשים. מודל שירותי הענן מאפשר לחברות וארגונים לצרוך משאבי מחשוב מגוונים ללא צורך ברכישת ציוד פיזי והתקנתו, במספר מודלים שונים:

- **תשתיות כשירות - Infrastructure as a Service (IaaS)**: מאפשר לארגון יכולות ניהול ופריסת משאבי מחשוב (אחסון, שרתים, רשתות, מערכות הפעלה וכו') בסיסיים. הארגון אינו מנהל או שולט בתשתית הענן הפיזית, אלא משתמש ביכולות אותן מחצין ספק הענן.
- **תשתיות תוכנה כשירות - Platform as a Service (Pass)**: מאפשר לארגון לספק, להפעיל ולנהל חבילות הכוללות פלטפורמות מחשוב (שרתים, אחסון, תקשורת) ויישומים, ללא המורכבות בתחזוקה של תשתיות פיזיות. הדבר מאפשר למפתחים לייצר חבילות שלמות המכילות את כל המרכיבים להפעלת היישומים שלהם.
- **תשתיות תוכנה כשירות - Software as a Service (SaaS)**: מאפשר לארגון יכולות החצנת יישומי תוכנה הניתנים כשירותים הזמינים לצרכן על פי דרישה, ספקי הענן מארחים ומנהלים את האפליקציה והתשתית הבסיסית שלה.

**תרשים 1 | מודלים להפעלת שירותי ענן**




ישנן כמה תצורות אפשריות לפריסת תשתיות הענן:

- **ענן ציבורי (Public Cloud)**: ענן ציבורי הוא הנפוץ ביותר מבין סוגי פריסות הענן. המשאבים מצויים בבעלותם ומופעלים על ידי ספקי שירותים של צד שלישי - כגון AWS או Google Cloud. ספק הענן הוא זה שמחזיק ומנהל את כל החומרה, התוכנה ותשתיות אחרות עבור לקוחותיו. משאבים אלו משותפים בין הדיירים של ספק הענן וניגשים אליהם באמצעים שונים (דפדפנים, סביבות פיתוח וכו'). הענן הציבורי מציע שירות אמין ביותר, על פי דרישה, ובעלות נמוכה יחסית, שאינו דורש תחזוקה מצד הצרכנים שלו.
- **ענן פרטי (Private Cloud)**: פריסת ענן פרטי פירושה, שהארגון מחזיק ושומר על משאבי מחשוב הענן שלו. משאבים אלה מאוחסנים בחוות השרתים של הארגון עצמו. היתרון המרכזי בגישה זו הוא, שהמשאבים מאוחסנים ברשת פרטית על חומרה ותוכנה ייעודיות, כלומר הארגון משיג שליטה, גמישות ומדרגיות משופרים בכל הנוגע לסביבת ה-IT שלו. החיסרון של המודל הזה הוא, שחברות המאמצות ענן פרטי אינן יכולות לממש במלואם את היתרונות של תשלום על פי שימוש - הן חייבות לשלם עבור התשתית מראש ולהמשיך לשלם עבור התחזוקה של מרכז הנתונים ללא קשר לרמות השימוש.
- **ענן היברידי (Hybrid Cloud):** פריסת ענן היברידי מתייחסת לשימוש משולב של תשתית ענן פרטית וציבורית. גישת ענן היברידי כוללת שימוש בכלי ניהול לביזור עומסי עבודה ולאיזון המשאבים של הארגון על פני עננים פרטיים וציבוריים. גישה זו גם מציעה לארגונים גמישות רבה יותר במעבר בין שתי שיטות הפריסה בהתאם לצרכים ולתקציב העומד לרשותם. עם זאת, סוג פריסה זה מוסיף מורכבות לסביבה הטכנולוגית של הארגון.
- **IT היברידי (Hybrid IT):** מודל פריסה זה משלב בין שירותי ענן עם פתרונות המתארחים בחוות השרתים של הארגון (On Premises). מודל זה נחשב למודל הפריסה הפופולרי ביותר (במיוחד בארגונים גדולים), כיוון שהוא מספק עלות-תועלת גדולה עבור ארגונים שכבר יש להם מערכות פועלות בסביבת ה-On Premises שלהם, ובנוסף מעוניינים לפרוס פתרונות ענן חדשניים במהירות.

כמתואר לעיל, המונח "ענן ציבורי", או "מחשוב ענן ציבורי", מתייחס למרכזי מחשוב ונתונים (Data Centers) של חברות מסחריות ברחבי העולם ולשירותי המחשוב המגוונים ללקוחות שונים באמצעות רשת האינטרנט. שירותי הענן מספקים פתרונות מנוהלים עם יתירות, שרידות, המשכיות עסקית ויכולת לתמוך בעומסים ובגידול בהיקף הפעילות בצורה דינאמית ללא צורך בהתחייבות לצריכה, תוך פישוט תהליכי הרכש והפחתת מורכבות התפעול ועלויותיו. במסגרת פרויקט "נימבוס", נבחרה תצורת ענן ציבורי עבור מעבר הממשלה לענן, ובהלימה לעיקרון cloud-first, כפי שמפורט בתפיסת ההפעלה לענן בפרק 5 למסמך זה. מטבע הדברים, ולאור מורכבות התהליך הטכנולוגי של שינוי תשתיות, מעבר משרדי הממשלה לענן ייעשה בהדרגה, כך שבתקופה הראשונה לפרויקט המשרדים יעבדו בתצורה היברידית, במטרה למקסם את היכולות הקיימות של חוות השרתים הפיזיות יחד עם היכולות המתקדמות שאותן יקבלו בעזרת ספקיות הענן. לאורך הזמן ועם הגירת המערכות הממשלתיות לענן, השימוש ביכולות הענן צפוי לגדול, ובכך להקטין ובחלק מהמקרים לייתר את הצורך בחוות שרתים פיזיות בניהול המשרדים, על המשאבים הכרוכים בהן.

## 2.2 ניתוח המצב הקיים

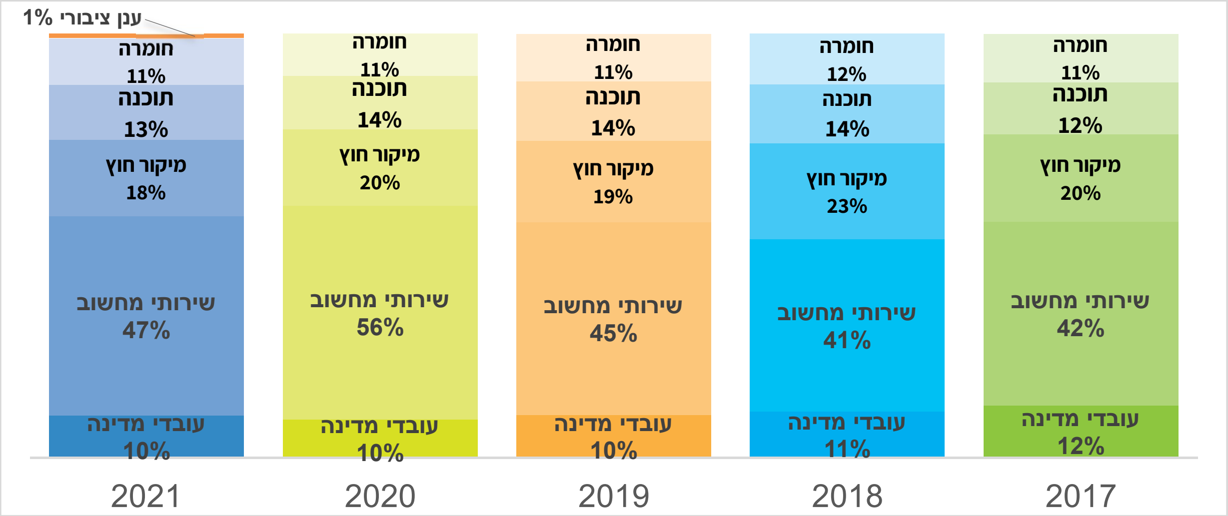
בדומה לארגונים מסורתיים אחרים (פיננסים, ביטוח וכו') מערכות ותשתיות המחשוב שהוקמו במשרדי הממשלה לאורך

העשורים האחרונים מתבססות לרוב על טכנולוגיות מיושנות בהיקפים נרחבים, המשמשות כבסיס למערכות הליבה של ארגונים ותהליכים עסקיים חשובים. בנוסף, חוסר ההיכרות והניסיון בשיטות וכלים טכנולוגיים חדשים מהווה פער מיומנויות משמעותי בכניסת טכנולוגיות חדשות ויכול להוות אתגר משמעותי. פער זה מתייחס הן לגורמים הטכנולוגיים והן לגורמים המקצועיים-עסקיים.

על אף ההתפתחות המהירה של טכנולוגיות IT ארגוניות בעשורים האחרונים, הממשלה מתקשה למנף אותה לתהליכים טכניים ועסקיים יעילים ורווחיים, כאשר הדרישה לעבודה אג'ילית (Agile), זריזה, מקבילית ומורכבת נתקלת בחסמים ארגוניים ובירוקרטיים, הנובעים, בין היתר, מאופייה המבוזר של הממשלה וממנגנוניה. מגמה זו תרמה למנטליות הסילואים בארגונים, המתבטאת בכך, שקבוצות ומחלקות מהססות לחלוק מידע ומשימות הן במשרדים עצמם והן לרוחב הממשלה. על מנת לייצר את החיבוריות והשיתוף הנדרשים, יש צורך ביצירת סטנדרטים, הנחיה מרכזית, מתודולוגיות, תהליכים סדורים ושימוש חוזר בשירותים ובפתרונות משותפים, בדגש על איגום משאבים לטובת ייעול ההשקעה במערכות מידע וטכנולוגיה.

מסמך סיכום פעילות התקשוב הממשלתי לשנת 2021[1] מצביע על ההשקעה הכלכלית של הממשלה בשירותי המחשוב השונים. ניתן לראות שכ-71% מהתקציב המיועד למחשוב מושקע בחומרה, בתוכנה ובשירותי מחשוב, בעוד השאר מושקע במיקור חוץ ובעובדי מדינה.

**תרשים 2** | השקעת הממשלה בשירותי מחשוב

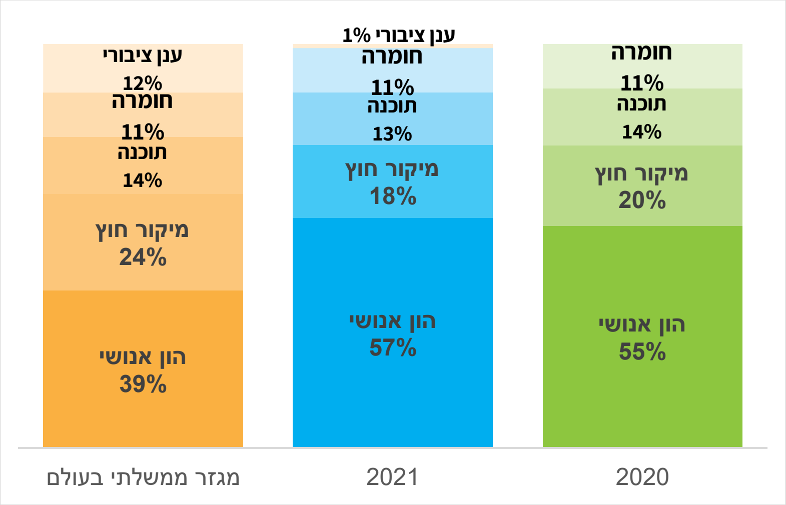



בנוסף, ניתן להתרשם, כי ההשקעה בטכנולוגיות ענן ציבורי בשנת 2021 הייתה כ-1% מהתקציב, בעוד שסך ההשקעה המקבילה במגזר הממשלתי בעולם עומדת על כ-12% מסך התקציב.

---

[1] תקשוב ממשלתי - מבט על פעילות 2020.

**תרשים 3** | השקעת הממשלה בטכנולוגיות ענן




הבדל משמעותי זה ברמת ההשקעה בפתרונות ענן ציבורי מדגיש את הצורך בתהליך סדור להדבקת הפער של הממשלה גם אל מול ממשלות אחרות בעולם, ולא רק אל מול המגזר הפרטי. בנוסף, היקפי השימוש וההוצאה על טכנולוגיה צפויים לעלות באופן יחסי במהלך השנים הקרובות, הן לאור תהליך המעבר לענן ותחזוקה מקבילה, והן בשל שיפור הנגישות לכלים ולמוצרים בענן, העתידים להגביר את היקף השימוש בטכנולוגיה.

בשנת 2018 ביצעה הממשלה הערכת מצב של מערכות המחשוב בממשלה לקראת מעבר לתצורות עבודה בענן. בתהליך זה נבחנו אפשרויות שונות של עבודה, שכללו ענן ציבורי, ענן פרטי, תצורת עבודה היברידית והשארת המצב הקיים. תהליך הערכת העלויות ובחינת החלופות העלה, כי שימוש בענן ציבורי מהווה החלופה המשתלמת ביותר, עם עלות משוערת של כ-2.8 מיליארד ש"ח על פני תקופה של 7 שנים. אף על פי כן, שימוש בתצורה היברידית של ענן נתפסת כאלטרנטיבה הישימה ביותר עבור ממשלת ישראל, מכיוון שהתצורה ההיברידית תומכת בענן ציבורי ובמודל של אירוח חלק מעומסי העבודה באופן מקומי (On Premises). העלות המשוערת של אלטרנטיבה זו הוערכה בכ-4 מיליארד ש"ח על פני תקופה של 7 שנים.

במקביל למהפכת המידע ולאור ההזדמנויות הטמונות בדיגיטל, משרדי הממשלה השקיעו בשנים האחרונות רבות באסטרטגיית מחשוב ודיגיטל. השקעה זו מביאה את משרדי הממשלה ויחידות הסמך לנקודת בשלות גבוהה לקראת קפיצת מדרגה ביכולות הדיגיטליות של הממשלה. בנוסף, כדי לשמור על עדכניות טכנולוגית על הממשלה לעבור לטכנולוגיות ענן, עמדה הנתמכת גם בניתוח כלכלי שנעשה לחלופות תצורות הענן, המצביעה על תצורה היברידית כפתרון המועדף. לאור זאת, פרויקט "נימבוס" יאפשר לממשלה לבצע את קפיצת המדרגה הנדרשת מבחינה טכנולוגית ועסקית.

## 2.3 פרויקט נימבוס

פרויקט "נימבוס" הוא פרויקט דגל רב-שנתי רחב היקף, המקודם על ידי מינהל הרכש הממשלתי ומערך הדיגיטל הלאומי, בשיתוף עם אגף תקציבים והלשכה המשפטית במשרד האוצר, מערך הסייבר הלאומי, משרד הביטחון, צה"ל וגורמים נוספים, במטרה לתת מענה מקיף לנושא אספקת שירותי ענן עבור ממשלת ישראל.

מתוך הראייה של "נימבוס" כפרויקט רחב, המקודם מתוך הסתכלות על מעגל החיים הכולל של שירותי ענן, הפרויקט כולל בשלב זה כמה רבדים מרכזיים:

- **רובד 1:** מכרז מרכזי לאספקת שירותי ענן ציבורי עבור משרדי הממשלה ויחידות הסמך – מכרז זה נועד ליצור את הערוץ המרכזי לאספקת שירותי הענן בפועל. במכרז זה זכו החברות Amazon Web Services (AWS) ו-Google כזוכה ראשון וזוכה שני, בהתאמה (להלן: "ספקי הענן").
- **רובד 2:** מכרז מרכזי למתן שירותי ייעוץ וליווי לצורך הקמה של ה-Cloud Center of Excellence והפעלתו. במכרז זה זכתה חברת סומך חייקין KPMG, אשר מספקת שירות ייעוץ בנושא.
- **רובד 3:** הוספת התמחויות במסגרת המכרז המרכזי לאספקת שירותי טכנולוגיות מידע בתפוקות במטרה לאפשר למשרדי הממשלה להתקשר עם מגוון חברות, אשר מוסמכות על ידי ספקי הענן לצורך קבלת שירותי ייעוץ, בחינה, תכנון, ליווי, עריכה של התאמות ומודרניזציה של אפליקציות בארגון וביצוע בפועל של הגירת הפעילות הארגונית לענן.
- **רובד 4:** רובד זה נועד לתת מענה לצורכי המשרדים בהיבטי בקרה תקציבית ואופטימיזציה פיננסית וטכנו-תקציבית של הפעילות הארגונית בענן ושל המערכות הפועלות בו, על ידי יצירת אפשרות להתקשר עם ספקים המתמחים בעולם תוכן זה וכן ליישם כלים, המשמשים לניטור ולבחינה של הפעילות הארגונית ועל ידי כך לנצל הזדמנויות לחיסכון ולייעול הפעילות.
- **רובד 5:** ספקי הענן מאפשרים ללקוחות לממש אלפי ואף עשרות אלפי שירותי צד ג' על גבי הפלטפורמות שלהם בין אם על ידי מימוש עצמאי של רישוי המערכת המסופקת על ידי ספק צד ג', ובין אם באמצעות ה-Marketplace שמפעיל ספק הענן. רכש שירותים מה-Marketplace של ספקי הענן מאפשר לממש על גבי פלטפורמת הענן, בקלות יחסית, מגוון רחב של שירותי צ ג'. רובד זה נועד להסדיר את אופן הרכישה של מוצרי צד ג' הניתנים לרכישה ב-Marketplace של ספקי הענן על ידי הוספתם לשוק דיגיטלי ייעודי, שיוקם עבור משרדי הממשלה, הוא השוק הדיגיטלי הממשלתי.

ספקי הענן הזוכים מקימים במדינת ישראל אזורים (Regions) במדינה שמהם יסופקו שירותי ענן ציבורי עבור ממשלת ישראל. כל אחד מהאזורים יכלול לפחות 3 מתחמים (Zones/Availability Zones), אשר ימוקמו בפיזור גיאוגרפי נרחב על מנת להבטיח עמידות, שרידות ורציפות תפקודית גם במצב של נתק תקשורתי מהעולם. נוסף על כך, כבר כעת מאפשרים ספקי הענן למשרדי הממשלה לצרוך מגוון רחב של שירותים מאזורים המופעלים על ידם בחו"ל. לצורך כך העמידו ספקי הענן אזורי ענן גדולים המופעלים על ידיהם באירופה – אזור אירלנד עבור AWS ואזורי הולנד ופרנקפורט עבור גוגל GCP – כאזורים זמניים, אשר ישמשו את משרדי הממשלה עד להשלמת ההקמה של אזורי הענן במדינת ישראל.

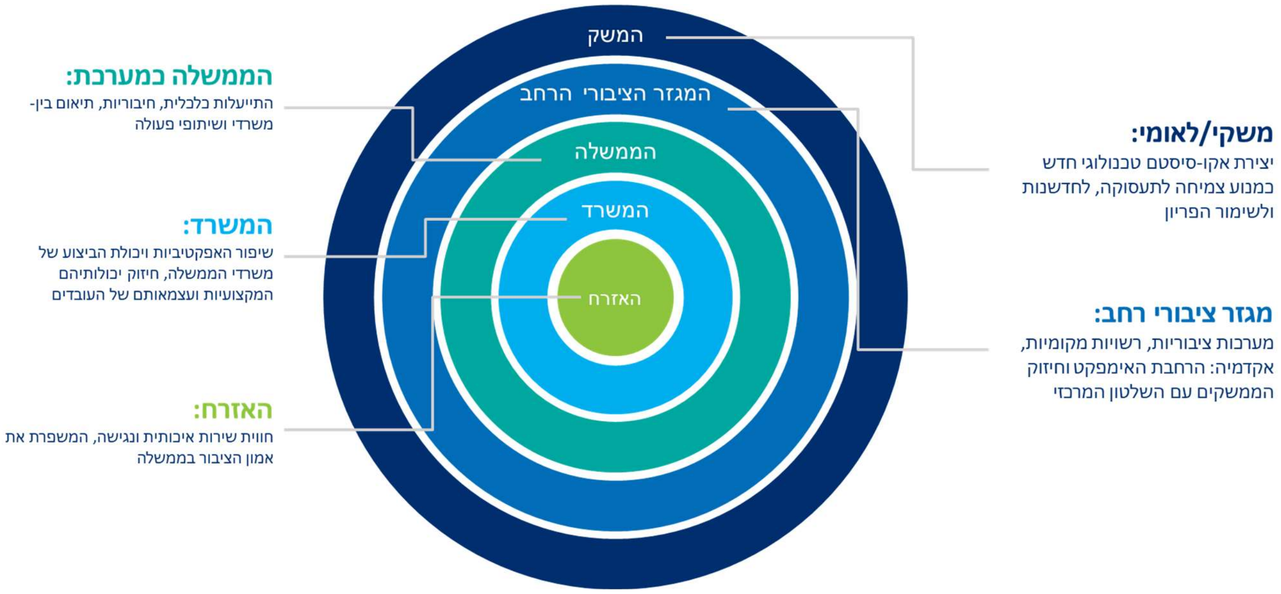
גישת ריבוי עננים, כפי שנבחרה בפרויקט "נימבוס", מאפשרת לארגונים יתרונות רבים, לרבות בחירה בין יכולות מימוש שונות וגמישות, שיפור עלויות ופתרונות מתקדמים המאפשרים למצות את הערך המוסף של כל אחד מספקי הענן הנבחרים. אחד היתרונות הגדולים ביותר של ריבוי עננים הוא הימנעות מנעילה על ספק או ספק שירות אחד, המאפשרת לארגונים לנצל את שירותיהם של מומחים המתמקדים בתחום מומחיות אחד או סוג אחד של יישומי ענן. גישת ריבוי עננים מאפשרת לארגונים לפרוס שירותים מרובים במקום להסתמך על ספק אחד עבור כל דרישות התוכנה שלהם. דבר זה מבטיח יכולת לפרוס את הפתרונות העדכניים ביותר, לספק את הסביבה בעבור מפתחי התוכנה כדי לבצע את עבודתם בצורה יעילה יותר, ולעבוד עם הטכנולוגיות העדכניות והטובות ביותר.

# 3 | חזון הענן הממשלתי ומרחב ההזדמנויות

הממשלה תאמץ שירותי ענן ציבורי מתקדמים במטרה לשפר את השירות לציבור, להגביר את האפקטיביות של המדיניות הממשלתית, להאיץ תהליכי חדשנות ולחזק את יכולותיו המקצועיות והטכנולוגיות של המגזר הציבורי, תוך קידום התייעלות כלכלית, מקסום הגמישות הטכנולוגית ושמירה על הגנה בסייבר ואבטחת מידע.

חזון הענן הממשלתי רואה בפרויקט "נימבוס" זרז לשינוי תהליכי עומק, המשפיעים על עבודת הממשלה בכל רבדיה, באמצעות היכולת לממש פתרונות טכנולוגיים לצורכיהם המקצועיים של המשרדים בצורה מהירה, מתקדמת ומדרגית (Scalable), המתאימה לקצב התדיר של השינויים בצרכים, באופן צריכת השירותים ובסדרי העדיפויות. מימוש מלא של החזון יוביל ל"אפקט אדווה", שגליו ישפיעו על כל היבטי הפעילות של הממשלה, על המגזר הציבורי הרחב ואף על המשק כולו.

**תרשים 4** | מעגלי ההשפעה




## 3.1 מרחב ההזדמנויות בענן

כפי שניתן להבין ממעגלי ההשפעה הנרחבים והרבים, פרויקט "נימבוס" והמעבר לענן הם בעלי פוטנציאל ליצירת אימפקט רב-ממדי וארוך טווח, המבוסס על ההזדמנויות החדשות הנפרסות בפני הממשלה. סעיף זה ממפה את ההזדמנויות האלה כרקע למיקוד אסטרטגיית הענן במטרות וביעדים נבחרים.

### 3.1.1 קפיצת מדרגה טכנולוגית:

יישום אפקטיבי של פרויקט הענן הממשלתי יאפשר קפיצת מדרגה בכל הקשור ליכולות הטכנולוגיות הממשלתיות ולשירותים הדיגיטליים הניתנים לציבור, הן כאמצעי לשיפור איכות השירותים הקיימים ולזמינותם והן כפלטפורמה לפיתוח סוגים חדשים של שירותים. זמינותם של פתרונות מתקדמים מהשורה הראשונה על גבי תשתית משותפת ומאובטחת, המנוהלת בצורה מרכזית, תוביל ליתרונות טכנולוגיים ניכרים עבור הממשלה:

- **גמישות וזמינות:** מחשוב ענן מאפשר להרחיב או להקטין בקלות את היקף שירותי ה-IT לפי הצורך, דבר המאפשר למשרדי הממשלה לתת מענה לצרכים משתנים לאורך זמן. לדוגמה, כאשר צפוי עומס של פניות לצריכת שירות מסוים, מוקצים משאבי מחשוב בהתאמה לצורך הנקודתי. בשימוש בשירותי ענן, מדרגיות (Scalability) זו מתאפשרת "בלחיצת כפתור" או באופן אוטומטי, לפי הצורך.

- **שיפור תפעולי:** מגוון השירותים על גבי פלטפורמת הענן והיקפם יובילו לצמצום הפער בין הדרישות העסקיות למענה הטכנולוגי באמצעות הגדלה של היצע הפתרונות הזמינים והיכולת לממשם מהר ובצורה איכותית במענה לצרכים משתנים, תוך קיצור זמני הפיתוח (Time to market).

- **חדשנות טכנולוגית:** יותר ויותר חברות טכנולוגיות מציעות כיום את שירותיהן בענן, ובהתאם למגמה הכללית - כבר בעתיד הקרוב יהיו שירותים אלו זמינים בענן בלבד. בנקודה זו, על מנת לצמצם את הפער הטכנולוגי ולהבטיח שמירה על עדכניות, על הממשלה לאפשר ולתעדף שימוש בענן כדי לצרוך שירותים הכרחיים לעבודתה. מעבר לכך, השילוב בין מגוון הכלים ונגישות השירותים בענן לבין זמינות כוח עיבוד ואחסון בלתי מוגבל, לצד פישוט תהליכי הרכש ומודלי שימוש מבוססי צריכה מאפשר יצירה של מרחב התנסות חדש עבור המשרדים בזמן קצר ותוך הפחתת מחיר הסיכון ובמחויבות נמוכה. היכולת להתנסות מאפשרת למידה תוך כדי תנועה וחדשנות מתמדת (Fail fast, learn fast).

חדשנות זו מתמקדת בתחומים הבאים: יישומי IoT (Internet of Things) הם בעלי פוטנציאל השפעה ניכר, בין היתר על עולמות התכנון, הביטחון והבטיחות במרחב הציבורי. יישומים אלו מבוססים על חיישנים ומכשירים אשר שולחים ומקבלים נתונים, אותם נדרש לאחסן, לעבד ולנתח בזמן אמת; יישומי למידת מכונה (Machine Learning) הם בעלי פוטנציאל השפעה על עולמות המחקר, האנליזה והתמיכה בקבלת החלטות. יישומים אלו מבוססים על לימוד המכונה על ידי גורמים אנושיים באופן שבו מלמדים בני אדם לזהות תבניות בנתונים, אלא שמכונות מסוגלות לבצע פעולות אלו על היקפים עצומים של מידע (Big Data) ובמהירות הקרובה לזמן אמת; יישומי Distributed Ledger (בלוקצ'יין) הם בעלי פוטנציאל לחולל מהפכה בעולמות של שרשראות אספקה, רישומי מעקב ובקרה המשותפים בין גופים הפועלים בסביבות תומכות (eco-system) רחבות (לדוגמה - שרשראות אספקה של תרופות/מזון/נדל"ן). הענן מהווה הבסיס לכל הטכנולוגיות האלו, ומעבר לעבודה בענן יבטיח, שניתן יהיה לעשות בהן שימוש בממשלה בהתאם ליעדיה.

- **שיפור יכולות ההגנה בסייבר:** השימוש בענן ציבורי מאפשר שיפור ברמת הגנת הסייבר ואבטחת המידע הן מבחינת שכבות ושירותי ההגנה המיושמים והן מבחינת היכולת לייצר מדיניות אבטחה רוחבית מוגדרת מראש, המונעת טעויות אנוש, שחלק נכבד מהן מהוות סיכוני סייבר. בנוסף, תפיסת הניהול המרכזי שאומצה על ידי הממשלה משפרת באופן ניכר את יכולתה של הממשלה להגיב לאיומי אבטחת מידע ברמה כלל-ממשלתית ובזמן קצר, תוך יצירת תמונת מצב בזמן אמת על כלל האיומים ומתן מענה להם.

- **התאוששות מאסון:** תשתיות הענן הציבוריות, המלוות בהסכמי רמת שימוש (SLA) ובהסכמי רמת תפעול (OLA),

משפרות את יכולתה של הממשלה להבטיח רציפות תפקודית ולצמצם את זמן השחזור ואת זמן ההשבתה של מערכות, תוך צמצום השיבושים העלולים להיגרם כתוצאה מכך. בנוסף, סביבת ענן מציעה פתרונות מבוססי אוטומציה וטכנולוגיה מתקדמת, המאפשרים התאוששות מהירה.

- **שקיפות ובקרה:** פלטפורמת הענן מאפשרת בקרה ומעקב אחר כלל התהליכים ומערכות המידע באמצעות תיעוד מפורט (logging), באופן המאפשר החלת סטנדרטים ומדיניות טכנולוגית, הגברת השקיפות על השימוש במשאבי הענן והבטחת יישום אפקטיבי של אמצעי הגנת סייבר.

### 3.1.2 התייעלות כלכלית:

עם הגידול המתמיד בהיצע השירותים הדיגיטליים שהממשלה מספקת, וביתר שאת עם הטרנספורמציה הדיגיטלית של השנים האחרונות, צפויים משרדי הממשלה להידרש לעמוד במשימות רבות יותר ולתת מענה לצרכים עסקיים נרחבים ומורכבים יותר. השימוש בפלטפורמת הענן, המבוססת על מכרז "נימבוס" ותנאי ההתקשרות שנקבעו בו, יובילו בטווח הארוך לחיסכון כלכלי משמעותי:

- **ייעול ההוצאה הממשלתית על תשתיות IT:** בטווח הארוך, המעבר לשימוש בתשתיות הענן יאפשר צמצום המשאבים הנדרשים לאירוח ואחסון מערכות באופן מקומי (On Premises) הן בתשתית טכנולוגית, הן בנדל"ן שעד כה הוקדש לחוות שרתים והן בהון האנושי הנדרש. יודגש, כי גם בראייה ארוכת טווח יהיו יישומים אשר מטעמי ביטחון, משילות והגנת סייבר לא יועברו לענן, או מערכות המבוססות על טכנולוגיות ישנות (legacy) שאינן מצדיקות את ההשקעה שבמעבר לענן, ואלו ימשיכו להתבסס על מעטפת האירוח וההגנה הנדרשת באופן מקומי, אך השאיפה היא לצמצם ככל האפשר את היקפם של יישומים אלו, בהתאם לעקרון cloud-first שנקבע כמדיניות הממשלתית (ראו פרק 5 למסמך זה - תפיסת ההפעלה).[2]

- **מעבר למודל תשלום לפי שימוש:** המעבר מהוצאות הוניות (CapEx) להוצאות תפעוליות (OpEx) תאפשר אספקת שירותים בהתנהלות חסכונית, תוך השגת המטרות בעזרת משאבים ומודלי שימוש גמישים ומבוססי צריכה, בהתאם לצריכה בפועל.

- **איגום משאבים:** השימוש בשירותים המנוהלים בצורה מרכזית, דוגמת פלטפורמת ניהול ענן מרכזית באמצעות אזור הנחיתה הממשלתי (landing zone), שימוש בתבניות ועוד, יוביל לאיגום משאבים, שיתוף ידע וצמצום הכפילויות הקיימות כיום, כאשר כל משרד ממשלתי נדרש לפתח, להקים ולתחזק תשתיות ושירותים כגון אלה באופן עצמאי. השירותים המשותפים יתמקדו במכנה המשותף למשרדי הממשלה ובשימושים והצרכים הנפוצים והגנריים ביותר, אשר לגביהם יש ערך מוסף לניהול מרכזי. בנוסף, שימוש בשירותים מרכזיים יוביל למקסום שימוש חוזר (reuse) במערכות, קוד ונתונים ממשלתיים וייצור חיסכון בעלויות פיתוח.

- **מיקוד בערך עסקי וביתרון היחסי:** כיום משרדי הממשלה נדרשים להתמודד עם פיתוח והטמעה של כלים טכנולוגיים הנותנים מענה לצרכים גנריים, דוגמת גיבוי, אנטי וירוס, יכולות פיתוח, פורטלים ארגוניים, ניהול משימות ופרויקטים ועוד. פלטפורמת הענן תאפשר גישה יעילה ופשוטה למגוון רחב של מוצרי מדף (commodity) ולפלטפורמות Low

---

[2] יודגש, כי הממשלה תמשיך להשקיע משאבים נאותים בהגנת סייבר גם בענן, בהתאם להחלטת הממשלה בנושא זה.

אשר יאפשרו למשרדים למקד את מאמציהם ומשאביהם, בדגש על המשאב האנושי, בפתרונות code/No code גנריים ו/או מותאמים (customized) לצרכים הייחודיים של הארגון ובקידום חדשנות.

### 3.1.3 שינוי ארגוני

מעבר הממשלה לענן טומן בחובו פוטנציאל טרנספורמטיבי לא רק לגבי התשתית הטכנולוגית, אלא גם לגבי דפוסי הפעולה, המיומנויות והתפקידים הקיימים בארגון. תהליך המעבר לענן דורש היערכות והשקעה ארגונית, המשלבת את היתרונות היחסיים הן של אגפי הטכנולוגיות הדיגיטליות והמידע והן של היחידות המקצועיות וגופי המטה לטובת רתימת הטכנולוגיה למימוש היעדים העסקיים של המשרד. לצד המשאבים הנדרשים לתהליך, המעבר לענן מהווה הזדמנות לשינוי דפוסים, לייעול שיטות עבודה ולחיזוק יכולותיה המקצועיות של הממשלה:

- **הגברת שיתוף הפעולה בין משרדי הממשלה (collaboration):** כיום, בהיעדר סטנדרטים ואחידות קיים קושי באיתור מידע וביצירת חיבוריות בין משרדים ומערכות שונות דווקא בעת שבה הממשלה נדרשת ליותר ויותר שיתופי פעולה בין-משרדיים. השימוש בפלטפורמת הענן, כולל יישום סטנדרטים אחידים, תבניות ושירותים משותפים, יוביל לשיפור בתאימות ובחיבוריות המערכות והמידע הממשלתי, יפחית את חסמי השיתוף הטכניים ויגביר את השקיפות והאמון בין משרדי הממשלה באמצעות איתור ומיפוי הנכסים הדיגיטליים.

- **קבלת החלטות מבוססת נתונים (Data Driven):** עולמות הדאטה בענן מפותחים במיוחד ומאפשרים לנצל את יתרונותיו היחסיים, החל בכוח העיבוד הנדרש לצורך יכולות ניתוח מתקדמות ובינה מלאכותית ועד כלים טכנולוגיים ייעודיים, המאפשרים שירות עצמי מלא ומנגישים יכולות ניתוח לקהלים ברמות שונות של אוריינות דאטה. פלטפורמת הענן תאפשר משילות מידע, שיתוף נתונים בין משרדים ושילובם עם נתונים מגופים חיצוניים, יכולות תחקור והצגה מתקדמות, וכל זאת במטרה לאפשר לממשלה קבלת החלטות אפקטיבית ומבוססת נתונים. בנוסף, המעבר לענן מייצר יכולות ניכרות לחיבור מידע בין מקורות, שעד היום היו מבוזרים וללא ראייה מתכללת, לטובת הפקת תובנות מצרפיות הן לקידום המטרות העסקיות של המשרדים והן לשיפור השירותים ויכולות ההגנה בסייבר.

- **התאמת ההון האנושי בממשלה לעידן הדיגיטלי:** המעבר לענן מייצר שינויי עומק בכל תהליכי העבודה הקשורים בטכנולוגיה, כגון רכש, ניהול תקציב, ניהול מערכות מידע ופיתוח מוצרים דיגיטליים. שינויים אלו הם "חלון הזדמנויות" לפיתוח המשאב האנושי בכלל, והטכנולוגי בפרט, הקיים והעתידי, להתאמת המבנה הארגוני ברמת המטה וברמת המשרד ולהגדרה מחודשת של התפקידים, יחסי הגומלין ותחומי האחריות הרלוונטיים, כך שישרתו את יעדיה של הממשלה ככלל, ואת יעדי הענן בפרט.

- **שיפור הנגישות של היחידות המקצועיות באמצעות קידום תפיסת שירות עצמי:** ככלל, המגמה הקיימת בממשלה היא לאפשר עצמאות מרבית למשרדי הממשלה ולעובדיה בשימוש בטכנולוגיה, ובהתאם לכך לקדם שירותים מבוססי שירות עצמי. המעבר לענן ציבורי מאפשר את הרחבת המגמה באמצעות גישה למגוון כלים ושירותים המיועדים ישירות למשתמשי הקצה, כגון שירותי SaaS לניהול משימות, ניתוח נתונים, הקמת אתרים ועוד. שירותים אלו מגבירים את נגישותם של גורמי המקצוע לטכנולוגיות חדשות, מפחיתים את התלות בגורם טכנולוגי מתווך, המהווה לעיתים צוואר בקבוק, וממחישים ומבססים את תפקידם של אגפי מערכות המידע כמאפשרים של חדשנות טכנולוגית.

- **שיפור המיומנויות הדיגיטליות:** לצד הגברת הנגישות לטכנולוגיות חדשות, וכחלק ממכרז "נימבוס", המעבר הממשלתי לענן מלווה בתוכנית הכשרות מקיפה ומעמיקה, הפונה לכלל קהלי היעד בממשלה, טכנולוגיים ועסקיים

כאחד. מהלך זה יאפשר גישה לעולמות ידע חדשים ורכישת מיומנויות בשני רבדים: עבור העובדים ונותני השירותים הטכנולוגיים יהווה הענן הזדמנות להכשרה מעשית בחזית הטכנולוגיה בנושאים, כגון ארכיטקטורת מערכות, פיתוח בסביבת ענן וניהול סיכוני סייבר; עבור עובדי היחידות המקצועיות יאפשר מערך ההכשרה התנסות בכלים ובפיתוח מיומנויות הכרחיות לעידן הדיגיטלי, כגון ניתוח נתונים, ניהול פרויקטים, ניהול מוצר ועוד. השילוב בין רבדים אלו יצמצם את הפער בין היכולות הקיימות בממשלה לבין המיומנויות הדרושות לה בראייה צופה פני עתיד.

- **שיפור האטרקטיביות של המגזר הציבורי:** המגזר הציבורי מצוי בתחרות עזה בתחום גיוס הון אנושי איכותי, ובפרט בתפקידים טכנולוגיים. במסגרת השינויים בשוק העבודה, עובדים בעלי מיומנויות גבוהות מצפים כיום ממקום העבודה לייצר הזדמנויות לחדשנות וליישום שינויים, וכן לאפשר להם לצבור ניסיון ולרכוש כישורים שיהיו רלוונטיים להמשך הקריירה. הודות לגישה לתשתיות ולכלים חדשניים, והדגש על הקניית מיומנויות לעובדים, המעבר לענן מהווה הזדמנות עבור הממשלה והמגזר הציבורי כולו למיצוב מחודש כמעסיק תחרותי.

### 3.1.4 מנוע צמיחה למשק הישראלי

כמתואר בתרשים 4, לפרויקט הענן הממשלתי יש השפעות מרחיקות לכת מעבר ליתרונותיו הישירים עבור הממשלה. לצד שיקולי הריבונות, השיפור התפעולי והיעילות שעמדו בבסיס המהלך, מוטיבציה נוספת להקמת הענן בשטח ישראל הייתה פוטנציאל ההשפעה על המשק הישראלי כולו באמצעות יצירת אקו-סיסטם טכנולוגי חדש ובהתבסס על כמה מחוללים מרכזיים:

1. **זמינות שירותים מקומיים:** החלטת הממשלה לבחור בפתרון מבוסס ענן ציבורי תגדיל באופן ניכר את נגישותם של שירותי ענן בישראל ותפחית חסמים לדיגיטציה בסקטור העסקי ובמגזרים נוספים באמצעות השימוש בתשתית המוקמת בארץ, ובכלל זה היבטי הריבונות ואבטחת המידע הייחודיים לפרויקט "נימבוס". כבר בימים אלו ניכרת התקדמות משמעותית בשימוש בענן בגופים כגון בנקים, קופות חולים, חברות ממשלתיות וכו', וזאת לאור הקמת האזורים בארץ והתחייבות החברות לפריסה נרחבת של שירותים.
2. **השקעת ספקיות הענן במשק הישראלי:** במכרז הענן הממשלתי "נימבוס" התחרו החברות הגדולות בעולם, ומתוכן נבחרו שתי ספקיות מובילות -- AWS ו-GCP, אשר התחייבותן להקמת אזור (Region) של ענן בישראל מוערכת בהשקעה של כ-13 מיליארד ש"ח בתשתיות, בהון אנושי, במרכזי פיתוח ובשירותים מקצועיים.
3. **ההוצאה הממשלתית על תהליך המעבר לענן:** במסגרת מכרז "נימבוס" תשקיע הממשלה מיליארדי ש"ח בשנים הקרובות בהגירת תשתיות ומערכות לענן הציבורי, לרבות השקעה בשירותים מקצועיים של תכנון וארכיטקטורת מערכות באופן ייעודי לענן.
4. **זירה חדשה לשיתופי פעולה בין הממשלה למשק:** היכולת להנגיש נתונים, תהליכים ומערכות ממשלתיות בצורה מהירה, פשוטה ומאובטחת תסיר חסמים לחדשנות ותאפשר הקמת זירה ייעודית להתנסות, למחקר ולשיתופי פעולה עם האקדמיה, עם חברות סטארט-אפ, עם ארגוני החברה האזרחית ועם המגזר העסקי. השילוב בין הידע הקיים באקדמיה ובשוק הפרטי ובין השקעת הממשלה בתמרוץ חדשנות וביצירת הפלטפורמות והכלים לבצע זאת בענן יאפשר מימוש אפקטיבי של יעדיה הכלכליים והחברתיים של הממשלה.

גורמים אלו, יחד ובנפרד, עתידים לייצר אקו-סיסטם הולך ומתרחב, אשר ישפיע על המשק בכמה היבטים מרכזיים:

- **שוק העבודה:** הקמת התשתיות על ידי הספקיות הזוכות, לצד היערכות הממשלה לשימוש בשירותי "נימבוס", ייצרה כבר בשלב ההיערכות מאות משרות בתחומי הליבה של הענן, כאשר הגיוס לתחומי הליבה על ידי ספקיות הענן והממשלה לבדן צפוי להוסיף באופן ישיר אלפי משרות חדשות ואיכותיות למשק בשנים הקרובות. בנוסף, עם הרחבת האקו-סיסטם לשימוש במשק, צפויות להתווסף עוד אלפי משרות בשנה בשירותים המשיקים לענן, לרבות שיווק, תמיכה, פיתוח ולוקאליזציה. זאת ועוד, התחייבות ספקיות הענן לספק עשרות אלפי ימי הכשרה להון האנושי בממשלה תתרום ליצירת משרות חדשות בתחום ההכשרות הטכנולוגיות וההסבה המקצועית לתחומי הליבה של הענן – בממשלה ובשוק האזרחי. חשוב לציין, כי כבר היום קיים מחסור חמור בהון אנושי טכנולוגי במשק, ובפרט בתחום הענן, ויש צורך בצעדים ברמה הלאומית על מנת לוודא, כי הזדמנויות התעסוקה שמייצר פרויקט "נימבוס" תמומשנה במלואן.

- **העלאת פריון העבודה במשק:** דיגיטציה היא גורם מפתח עבור עסקים להתייעלות בתהליכי עבודה, הוזלת עלויות תפעוליות, מיקוד וייעול של השקעות הון בתחום ה-IT ושיפור השירותים ללקוחותיהם. נגישות המשק לריבוי הכלים והטכנולוגיות הזמינות בענן, ובפרט נגישותם של עסקים קטנים ובינוניים ותעשייה מסורתית, תפחית חסמי כניסה, תוזיל ותקל את יכולתם לאמץ חדשנות ולהטמיע שירותים דיגיטליים מתקדמים. זאת ועוד, הענן ייתן מענה למגזרים בעלי אופי ציבורי, או כאלה הנתונים לרגולציה ייעודית, כגון בנקאות, פיננסים או בריאות, אשר מטעמי ריבונות והגנת המידע מוגבלים ביכולתם להשתמש בשירותי ענן הממוקמים בחו"ל. מגזרים אלו יוכלו גם הם ליהנות מיתרונותיו של ענן ציבורי הממוקם בארץ ולמנף את הכלים והשירותים המתקדמים שהענן מציע לטובת שיפור ביצועים.

- **מיצוב מדינת ישראל כמובילה עולמית בתחום הענן:** ל"נימבוס" פוטנציאל להפוך את מדינת ישראל לאחת המובילות העולמיות בטכנולוגיות הליבה של הענן. הזמינות הטכנולוגית, המהירות, הנגישות, התמיכה הטכנית בעברית, ההון האנושי הטכנולוגי המתאים, השימוש הרחב הצפוי במשק, המשקיעים בתחום ועוד – ייצרו אקו-סיסטם שיזין וירחיב את עצמו לכדי מוקד ידע וזירת חדשנות עולמית, ההולמים את מעמדה של ישראל כ"אומת הסטארט-אפ". התחומים שצפויים להתפתח ולצמוח הם: שימושים מתקדמים בדאטה ובמידע, נצילות אנרגטית ואנרגיה ירוקה, תשתיות תקשורת ועוד.

בהמשך לגיבושה של אסטרטגיית המעבר לענן, תציג ממשלת ישראל תוכנית לאומית לעידוד הפיכתו של "נימבוס" למנוע צמיחה עבור המשק הישראלי. מניסיון העבר, במדינות שהוקמו בהן תשתיות ענן ציבורי רחבות כפי שמוקמות בישראל, דוגמת קנדה, בריטניה והודו, ההזדמנויות החיוביות המתוארות לעיל התממשו. חשיבות התוכנית הממשלתית לעידוד מגמות אלה היא בהיותה "מכפיל כוח" להזדמנויות המתוארות. זאת ועוד, תפקידה של התוכנית היא לכוון את התועלות הצפויות לטובת השגת מטרותיה של הממשלה בהקשרי החברה והכלכלה הישראלית.

# 4 | אסטרטגיית הענן הממשלתית – מטרות ויעדים

המטרות והיעדים של אסטרטגיית הענן הממשלתית נגזרים מהיקף ההזדמנויות הנרחב שמאפשר הענן, אך מתמקדים בשלב הראשון בהיבטים ההכרחיים של המעבר של משרדי הממשלה ויחידות הסמך לשימוש בענן, בהתאם לבשלות התחום במשרדי הממשלה, וזאת על מנת להבטיח את מיקוד המאמצים לטובת הצלחת האסטרטגיה. מטרות ויעדים אלו מתמקדים, ראשית, בפריסת התשתיות הקריטיות, בתהליכי העבודה ובתועלות הראשוניות לטובת הרחבת היקף השימוש בענן ובתכנון מעבר מקצועי ומתודולוגי, שיאפשר לנצל את יתרונותיו. בשלב מתקדם יותר ביישום הפרויקט, לאחר מעבר מסה קריטית של מערכות וארגונים לענן והתייצבות התהליך, תבחן הממשלה הרחבה של מטרות, יעדים ומשימות למעגלי השפעה נוספים, בדגש על היבטים משקיים, או הטמעה במגזר הציבורי הרחב.

## 4.1 שיפור השירותים והמוצרים הדיגיטליים לציבור (אזרחים ועסקים)

- קיצור זמני פיתוח של שירותים חדשים (Time to Market).
- שיפור הזמינות, האיכות והעדכניות של המוצרים הדיגיטליים שהממשלה מספקת.
- שיפור הגמישות והמדרגיות (Scalability) של הממשלה במענה לצרכים משתנים.

## 4.2 קפיצת מדרגה ביכולותיה הטכנולוגיות של הממשלה

- הרחבה של היקף השימוש הממשלתי בענן.
- ניצול אופטימלי של יכולות הענן.
- אימוץ והתנסות בטכנולוגיות חדשות.
- שוק דיגיטלי ממשלתי מגוון, איכותי, רחב ומוגן סייבר לשימוש המשרדים.

## 4.3 שיפור האפקטיביות וייעול ההוצאה הממשלתית בתחום הטכנולוגיה

- התאמה של תהליכי הרכש לקצב התפתחות הטכנולוגיה.
- שיפור של תהליכי הניהול הפיננסי בממשלה בתחום ה-IT.
- שימוש חוזר (reuse) במשאבים טכנולוגיים, דוגמת תבניות, קוד ונתונים.
- איגום משאבים באמצעות שימוש בשירותים משותפים בענן.

## 4.4 חיזוק היכולות המקצועיות של הממשלה

- שיפור שיתוף הפעולה והחיבוריות במרחב הממשלתי.
- קידום עבודה מבוססת נתונים במשרדי הממשלה.
- שיפור המיומנויות הטכנולוגיות והדיגיטליות של ההון האנושי בממשלה.
- שיפור הנגישות של יחידות מקצועיות לכלים דיגיטליים מתקדמים.

## 4.5 הבטחת המשילות, הריבונות וההגנה בסייבר על התשתיות הטכנולוגיות והמידע הממשלתי בענן

- קידום השימוש בתשתית ענן ציבורי מוגנת סייבר ואיכותית באזור ישראלי.
- חיזוק המשילות בתחומי הטכנולוגיה וההגנה בסייבר.
- יצירה והגדרה של מסגרת מדיניות, סיווג מערכות ומידע, ניהול סיכונים וקווים מנחים לשימוש ממשלתי בענן ציבורי.

# 5 | תפיסת הפעלה לענן בממשלה

מטרת פרק זה היא לתרגם את המטרות והיעדים של הענן המוגדרים בפרקים הקודמים של מסמך האסטרטגיה לכדי עקרונות אופרטיביים וכיווני פעולה המקדמים את הגשמתם. מתוך ראיית המעבר לענן כפרויקט אסטרטגי, המשרת את כלל מנגנוני הממשלה, תפיסת ההפעלה למימושו מבוססת על שיתוף פעולה מקצועי עם כלל בעלי העניין והשותפים, המהווים חלק אינטגרלי במהלך: בראש ובראשונה, משרדי הממשלה ויחידות הסמך, שהם מובילי מהפכת הענן ומימושה בפועל באמצעות אגפי טכנולוגיות דיגיטליות ומידע (טד"מ) - מנוע ההצלחה של אסטרטגיית הענן הממשלתית. לאגפי טד"מ תפקיד ייחודי ומכריע במעבר הממשלה לענן, החל מהובלת המהלך ברמה הניהולית למימושה של אסטרטגיית הענן במשרד ויצירת תוכנית פעולה ישימה, עבור ברתימת השותפים, בהבנת הצרכים העסקיים וביצירת ערך עבור כל הגורמים הרלוונטיים במשרד, וכלה בהעמדת הכלים הטכנולוגיים והתשתיות הנדרשות למימושה של תוכנית הפעולה.

לצד המשרדים, המעבר לענן מושתת על הובלה מקצועית של מערך הדיגיטל הלאומי ומינהל הרכש הממשלתי, בשיתוף הדוק עם גורמי המטה בממשלה, ובהם משרד ראש הממשלה, הממונה על התקציבים במשרד האוצר, החשב הכללי ומערך הסייבר הלאומי.

התפיסה המפורטת להלן מבוססת על הגדרה של עקרונות פעולה לכל אחד מהיבטי הניהול של המעבר לענן, התומכים ביוזמות האסטרטגיות שמובילים כלל הגורמים השותפים למימושו.

## 5.1 מרכז מצוינות מקצועי לענן - Cloud Center of Excellence

רוחב היריעה של נושא הענן בכלל והענן בממשלה בפרט מחייב תפיסת הפעלה מקיפה, המביאה בחשבון את מכלול היבטי השינוי הכרוכים במהלך זה – טכנולוגית, עסקית וארגונית.[3] לצורך יצירה של תפיסת הפעלה הוליסטית ומימושה הוקם מרכז מצוינות מקצועי לענן - ה-Cloud Center of Excellence (להלן: "CCoE"). ה-CCoE הוא גוף המורכב מכלל הגורמים הממשלתיים השותפים למהלך ופועל בתפיסה מטריציונית באמצעות צוותים חוצי-תחומים וארגונים, ומטרתו להוות גורם מאפשר למשרדי הממשלה באמצעות כמה תפקידי מפתח:

- הובלת יישומה של האסטרטגיה הממשלתית לענן, תיאום וסנכרון בין הגורמים השותפים, תעדוף יוזמות, איסוף מידע ושיתוף נכסים/תוצרים/מידע/תובנות, מדידה ובקרה של עבודת הממשלה בענן במסגרת המדיניות המוגדרת ובהתאם למטרות, ליעדים ולמדדים שהוגדרו ועדכון/התאמת היעדים והמטרות בהתאם לשינויים הנדרשים.
- גורם מייעץ, המסייע למשרדי הממשלה "לנווט" בעולם הענן, באמצעות הנגשת ידע, כלים, שיטות, מתודולוגיות וכו' לצד ליווי בביצוע של הקמת שירותים ומערכות חדשות בענן ושל העברת יישומים קיימים ("מיגרציה") לענן.

[3] תפיסת ההפעלה לנושא הגנת הסייבר מפורטת בפרק 7 למסמך זה, במסגרת תפיסת ניהול הסיכונים.

- תכנון מרכזי באמצעות איסוף צרכים, הגדרת דרישות, תעדוף והנחיה של צוותי הענן והארכיטקטים העוסקים בפיתוח שירותי IT משותפים, כפי שייקבע במסמכי מודל ההפעלה.
- מינוף וחשיפה של תחום הענן בממשלה, באמצעות עבודת שטח מול משרדי הממשלה ושילוב פעילות ארגונית תומכת (ראו היבטי ניהול השינוי בסעיף 6.4 למסמך זה).

יצירת מוקד ניהולי מתכלל מאפשרת ראייה רוחבית ואסטרטגית בכל הקשור לניהול הענן הממשלתי. תהליך עבודה זה מאפשר פתרונות טכנולוגיים ומדיניות, התואמים את צורכי המשרדים השונים ואת תפיסות ההפעלה הפרטניות לגבי מימוש הענן, סנכרון בין היבטי המימוש השונים וחיבור למטרות והיעדים המקצועיים של הממשלה, תוך יצירת ערך עבור הממשלה בטווח זמן קצר-מיידי. בנוסף, ניהול המהלך בידי גוף מרכזי יאפשר מדידה ובקרה שוטפת של התקדמות הפרויקט לצורך התאמתו לצורכי הממשלה ברמה הטכנולוגית והעסקית. בנוסף, ה-CCoE ילווה את משרדי הממשלה לאורך כל מחזור חיי המערכות מבוססות תשתיות הענן, בתהליכי הטמעת Best Practices, יערוך בקרה על עמידה בהגדרות הרגולציה ויאפשר בחינה כוללת בראיית מאקרו של השימוש וההוצאות הנדרשות על הסביבות השונות.

## 5.2 עקרונות למימוש טכנולוגי

מטבע הדברים, התחום שבו הענן מחולל את השינוי היסודי והעמוק ביותר הוא התחום הטכנולוגי על היבטיו השונים. במובן זה, מעבר הממשלה לענן משנה לא רק את המימוש הפיזי באמצעות חוות שרתים ואת האחריות לתפעול שכבות היישום השונות, אלא מייצר גם שינויים טקטוניים בתהליכי העבודה, הניהול והיישום של טכנולוגיות בארגונים. על מנת לתמוך בשינוי מורכב זה, העקרונות שלהלן, המעוגנים גם בהחלטת ממשלה מס' 231, מתווים את התפיסה ואת המסגרת האופרטיבית, שתסייע לממשלה לממש את יתרונות הענן תוך התייחסות למורכבות השינוי הטכנולוגי.

### 5.2.1 ענן תחילה (Cloud First)

כפי שנקבע בסעיף 1 בהחלטת הממשלה מס' 231, משרדי הממשלה ישתמשו בשירותי הענן כברירת מחדל (Cloud First) בבחירת פתרונות טכנולוגיים, ויש להעדיפם, ככל האפשר, על פני כל פתרון טכנולוגי אחר. תינתן העדפה לתפיסת מימוש הכול כשירות (Everything as a Service) - תפיסה שמעדיפה שימוש בשירות בכל מקום שניתן לעשות זאת, שבמסגרתה יש עדיפות למודל תוכנה כשירות (Software as a Service – SaaS) היכן שהדבר אפשרי ומספק מענה הולם לדרישות הפונקציונליות. היכן שיש צורך לפתח תוכנה – העדיפות היא לפתח במודל פלטפורמה כשירות (Platform as a Service – PaaS).

**תועלות:**

- יישום שירותים בענן בגישת "הכול כשירות" יאפשר למשרדי הממשלה להתרכז ביתרונות היחסיים ובהתאמת הפתרונות לצרכים העסקיים של הלקוחות, תוך הפחתה של השקעת התשומות בתשתיות, בתחזוקה שוטפת של מערכות שנקנו באופן חד-פעמי והותקנו בשרתים מקומיים, או בפיתוח פנימי של מוצרים.
- המשך פיתוח, עדכון והתאמה של המערכות באופן שוטף כחלק מהשירות ללא צורך בהשקעה נוספת מצד

המשרד.

הקטנת התלות בתשתיות טכנולוגיות אשר יוצאות משימוש (End of Life).

מעבר מהקמת יישומים וניהול תשתיות מחשוב למוצרים המסופקים כשירות ומתמקדים בצורכי משתמשי קצה.

מתן מענה תואם בהתאם לצרכים הגדלים ומשתנים של האזרחים, גמישות בצורכי המערכות השונות (Scale Up & Down) והבטחת הזמינות והאמינות של שירותי המחשוב כדי לשמור על אמון האזרחים בממשלה.

### 5.2.2 הגירה לענן (מיגרציה)

בהתאם למדיניות שנקבעה בסעיף 6 בהחלטת הממשלה מס' 231, על משרדי הממשלה לבחון את כלל המערכות הקיימות, לתכנן ולבצע הגירה שלהן לענן. שלב תכנון ההגירה הינו שלב קריטי בתהליך, שיתווה את אופן הביצוע ויכלול הערכה עסקית וכלכלית של תהליך ההגירה לענן. שלב זה יכלול תהליך של גילוי מצב קיים ארגוני, בחינת המערכת והתאמתה לתצורה ענניתׂ (cloud suitable), בחינת אופן ההגירה ובחינת של השקעת המשאבים שתידרש לכך. תהליך זה יאפשר למשרד לבצע "חריש עמוק", לבחון את הנכסים הקיימים בארגון (תשתיות, מערכות, דאטה) ולקבל החלטה עסקית וטכנולוגית על הגירת המערכות לענן.

תהליך המעבר לענן יתבצע תוך שמירה על כמה עקרונות בסיסיים ועל פי סדר העדיפות הבא:[4]

1. דרך המלך למעבר לענן היא תכנון פתרון אופטימלי למודרניזציה ולטרנספורמציה של המערכות לסביבות הענן, הכולל, בין היתר, שדרוג תשתיות של מערכות ושימוש בשירותים מנוהלים.
2. במקרה שנדרש מעבר מהיר לתשתיות ענן, המשרד ישתמש בעקרון Lift-and-Optimize, אשר במהלכו יתבצעו פעולות לייעול התשתיות אשר בשימוש המערכת בענן.
3. יש להימנע מחלופת Lift-and-Shift (המכונה Rehost), המספקת פתרון אירוח בלבד (לרוב במודל תשתית כשירות - IaaS), למעט במקרים שיש לכך הצדקה מיוחדת, כגון סגירת חוות שרתים, סיום חוזה מול ספק או התיישנות של ציוד, וגם אז יש לממש חלופה זו תוך תכנון אופרטיבי למודרניזציה או לאופטימיזציה של המערכות.

**תועלות:**

פוטנציאל לחדשנות ולהרחבת היכולות במסגרת הרחבה ותחזוקה של מערכות קיימות.

זיהוי הזדמנויות למודרניזציה ולטרנספורמציה (שינוי יסודי של מערכות ותהליכים ובנייתם מחדש תוך שיפור המענה לצורך העסקי), תוך ייעולן של מערכות המידע וניוון מערכות המבוססות על טכנולוגיות מיושנות

---

[4] עקרונות לתעדוף של הגירת מערכות לענן מפורטים בהנחיית מערך הדיגיטל הלאומי בדבר "היערכות משרדית למיגרציה לענן" מיום 16 בפברואר 2022 וכן במסגרת ההנחיות השוטפות שיוצאי ה-CCOE. אלה עתידות להתעדכן מעת לעת ותכליתן לתת מענה רחב ככל הניתן שיאפשר לכל משרד ויחידה לייצר תעדוף המותאם עבורם.

היוצאות משימוש (end-of-life).

בחינה מחודשת של נושאים אשר בעבר הוגדרו לא מעשיים או לא פתירים במטרה לאפשר פעילות אופטימלית של המערכות, כגון יכולת גידול לפי הצורך, הרחבה ותמיכה בעומסים (גם נקודתיים או פתאומיים), גיבוי ושרידות משופרים.

חיסכון והפחתה של עלות הבעלות הכוללת על מערכות המידע בארגון (TCO – Total Cost of Ownership).

### 5.2.3 יישום תפיסת "אזור נחיתה בענן" (LANDING ZONE)

"אזור נחיתה בענן" מהווה מעטפת תפעולית מנוטרת ומנוהלת על ידי גורם מרכזי, בין אם רוחבי או פנים-ארגוני, האחראי על מדיניות ההפעלה בענן ועל החצנת כלים ושירותים שונים בקטלוג שירותים, תוך עמידה בהנחיות ובדרישות השונות. שיטת עבודה זו תאפשר למשרדים להתרכז ביצירת פתרונות טכנולוגיים חדשים ללקוחותיהם, תוך מיקוד בצרכים העסקיים השונים. תפיסת "אזור נחיתה" כגישה להפעלת ענן מאפשרת, באמצעות נקודת כניסה אחת, מאובטחת, מנוטרת ומנוהלת, להסיר חסמים קיימים בהקמה וביצירה של שירותים ומוצרים חדשים ולפצות על כך באמצעות נוהלי בקרה.

**תועלות:**

הבטחת משילות, עמידה בנהלים, ציות להנחיות הגנה בסייבר, תאימות ואחידות בכל יישומי הארגון, כגון בשימוש בכלי פיתוח, בדיקה, ניטור, תחזוקה, תפעול, ניהול הייצור ועוד.

קידום עצמאות ברכישת כלים או בהקמת שירותים על ידי משתמשי הקצה, תוך הסתמכות על מדיניות מוגדרת ומנוהלת בצורה מרכזית על ידי הגורם הטכנולוגי.

### 5.2.4 מדיניות מרכזית תוך שמירה על עצמאות תפעולית

יישום המערכות הממשלתיות ייעשה בתצורת Multiple-Enterprise, Multiple-Cloud על גבי תשתיות הענן, שעליהן יופעלו שירותים מרכזיים ממשלתיים. מערך הדיגיטל יספק שירות ממשלתי משותף של ניהול וניטור של תשתיות ענן מרכזיות, אשר במסגרתו יופעלו לטובת משרדי הממשלה ויחידות הסמך "אזורי נחיתה" (ראו סעיף קודם – יישום תפיסת "אזור נחיתה בענן"), הפועלים על גבי התשתית של שתי ספקיות הענן הזוכות במכרז. ככלל, משרדי הממשלה ישתמשו בשירות אזור הנחיתה המשותף למעט במקרים חריגים – אשר לגביהם הוגדרו קריטריונים כאמור בהוראת התכ"ם מס' 16.2.2. פרויקט נימבוס - אספקת שירותי ענן ציבורי. למשרדי הממשלה תתאפשר עצמאות תפעולית במסגרת השימוש בשירותים המרכזיים הממשלתיים, ולצידה תינתן האפשרות להקים שירותים ארגוניים עצמאיים על גבי תשתיות הענן, בכפוף לעמידה במדיניות, בסטנדרטים ובנוהלי השימוש בענן בכל ההיבטים, ותוך התחייבות להקצאת היכולות המקצועיות והמשאבים הרבים הנדרשים לכך. תפיסה זו מעוגנת גם בסעיפים 4-5 להחלטת הממשלה מס' 231, המפרטים את התשתיות הנדרשות להקמה מרכזית בענן הציבורי ואת ייעודן כשירות רוחבי.

**תועלות:**

סטנדרטיזציה ביישום מדיניות הגנת הסייבר בענן, ניהול זהויות והזדהות, ניהול שירות, ניהול לוגים ובקרות.

ייעול וחיסכון בעלויות ההקמה של תשתיות תפעול וניהול ענן באמצעות ניהול מרכזי.

חיזוק המשילות בעזרת יצירת תבניות אחידות לשימוש משרדי הממשלה בעולמות אבטחת המידע, התשתיות, והפיתוח.

יצירת מסגרת, כלים ותהליכי עבודה, המאפשרים למשרדי הממשלה להתמקד ולהתמקצע בעולם התוכן העסקי וביתרון היחסי הייחודי להם.

### 5.2.5 אוטומציה בתהליכים ובמשימות תשתית

הכלים והיכולות הזמינים בענן יאפשרו טרנספורמציה של יוזמות הפיתוח בממשלה על ידי הטמעת תהליכי DevOps, המאפשרים למשרדי הממשלה יכולות מגוונות ומתקדמות, כגון ניהול ובקרת תצורה, ניהול שינויים במערכות וכן תהליכים אוטומטיים בעת קידום התוכנה בשלבי מחזור החיים מפיתוח לבדיקות ולייצור. כיוון שרבים מכלי האוטומציה מותאמים לתצורת העבודה בענן ומובנים בה, הכנסת תהליכים אלו מעשית יותר בעת מעבר המשרדים לענן לעומת יישומם במערכות המנוהלות On Premises.

**תועלות:**

ייעול של תהליכי פיתוח באמצעות תהליך רציף בין צוותי הפיתוח לתחזוקה, הגדרת תהליכים ומשימות החוזרים על עצמם והקטנת התלות בפעולות ידניות. קיצור של מחזורי פיתוח התוכנה תורם להגברת האג'יליות (Agility), תוך קיצור משמעותי בזמני הפיתוח ובמענה לדרישות משתמשים.

ניהול של משאבי הארגון בצורה פשוטה ויעילה בעזרת תבניות מוגדרות ותהליכי אוטומציה (לדוגמה, הקמת תשתיות חדשות, עדכון מוצרי אבטחה על המערכות, פרסום ושדרוג של שירותים לצרכנים וכו').

יכולות אבטחה מתקדמות באמצעות כלים המשולבים בתוך תהליכי האוטומציה, המנהלת את מחזור חיי התוכנה (DevSecOps).

### 5.2.6 שיתופיות (Collaboration)

בתהליך המעבר של הממשלה לענן תינתן עדיפות לפלטפורמות, לכלים, ולשיטות עבודה התומכים בשיתופיות (collaboration). טכנולוגיות הענן מבוססות על עבודה עם תשתיות וכלים בסטנדרטים אחידים, המאפשרים שיתוף קוד בצורה יעילה ומשפרים את זמינות הנתונים ואת נגישותם באופן התומך בפירוק הסילואים הטכניים והקונספטואליים הקיימים, הן בין משרדי הממשלה והן בתוך הארגונים עצמם. כך, לדוגמה, אירוח הנתונים הממשלתיים על גבי תשתית ענן משותפת מאפשר שיתוף נתונים בהתבסס על תפיסת ניהול סיכונים באמצעות כלים מתקדמים לניהול הרשאות במקום שכפול והעברה פיזית של נתונים כפי שמתבצע כיום. בנוסף, פיתוח תוכנה באמצעות כלים ומאגרי קוד בענן פותח הזדמנות לשיתוף קוד במרחב הממשלתי לצורך שיתוף והעברה של ידע וכן להפצת פתרונות שפותחו במשרד אחד לטובת כלל המשרדים, בדומה לעולם הקוד הפתוח.

**תועלות:**

אחידות ושימוש חוזר בקוד, גם כזה שנכתב על ידי המשרד עצמו, וגם כזה שנכתב על ידי משרדים אחרים.

ייעול וחיסכון בתהליכי פיתוח של מערכות חדשות ושיפור מערכות קיימות באמצעות שקיפות ומשוב.

הרחבה של מנעד הכלים והשיטות והתמקצעות טכנולוגית של משרדי הממשלה באמצעות שיתוף ידע.

שיפור היכולת לממש פרויקטים בין-משרדיים בקלות ובמהירות.

שיפור היכולת לגשת למשאבי המשרד מכל מקום ובכל זמן, ובכך לתת מענה לסביבות עבודה היברידיות בהתאם לצרכי הארגון וכמענה למציאות משתנה.

## 5.3 תפיסת הפעלה לניהול פיננסי בענן

ניהול פיננסי נכון של הפעילות הארגונית בענן הוא חיוני על מנת להבטיח עבודה יעילה ומיטבית של הארגון בענן. אחד היתרונות המרכזיים בניהול מערכות בענן הוא שקיפות מלאה של כלל ההוצאה הארגונית על IT והאפשרות לשייך כל הוצאה לתהליך, לפרויקט ולשלב במחזור החיים של המערכת. הדיסציפלינה של Cloud FinOps נועדה לייצר פרקטיקה, שמטרתה לאפשר לארגונים למקסם את הערך העסקי (התועלת) הנובע מהשימוש בענן. עולם ה-FinOps הוא רחב ומורכב ומשלב היבטים כלכליים, טכנולוגיים, עסקיים ותפעוליים. תהליך FinOps איכותי רותם את מירב הכלים והתועלות משני עולמות תוכן מרכזיים – תקציבי/פיננסי וטכנולוגי, ומצריך הבנה מעמיקה של טכנולוגיות ענן, היכרות עם סוגי השירותים, מבנה העלויות, מנגנוני תמחור, מתווה השימושים והצריכה של המזמין, וכן היכרות עם מפת הדרכים (Roadmap) של ספקי הענן ביחס לשירותים ולמודלי צריכה שונים.

על מנת לבצע את תהליך הניהול הפיננסי בענן באופן מוצלח יש צורך בשילוב של הנחיות וכלים הן ברמה על-משרדית והן ברמה המשרדית עצמה. ברמה העל-משרדית, היות שהניהול הפיננסי בענן כולל בתוכו היבטים של חשבונאות לאומית, יש צורך לייצר הנחיות ברורות וסדורות, אשר יאפשרו את המימוש בפועל של הנחיות מרכזיות, כדוגמת קביעת מדיניות תיוגים (Tagging). ברמה המשרדית, יש צורך לייצר תהליכי עבודה סדורים בתוך המשרד על מנת להבטיח שתהליך הניהול הפיננסי בענן יביא ערך משמעותי לארגון הן מבחינה תקציבית והן מבחינה תפעולית.

תהליך הניהול הפיננסי בענן מתבסס על העקרונות המפורטים להלן:

- **ליווי בתהליכי הבחינה הפיננסית של הפרויקטים המקודמים:** קביעת הנחיות ובקרה למול הגורמים הטכנולוגיים והיחידות העסקיות הדורשות ביחס לאופן מימושם וניהולם השוטף של פרויקטים בענן.
- **שילוב של תהליכי התכנון הפיננסי בעבודה הארגונית הטכנית:** שילוב היבטים פיננסים בתהליכי תכנון ארכיטקטורה, בחינה של טכנולוגיות שונות ועריכת אופטימיזציה טכנית כדי למטב את עלויות השימוש בענן ולמקסם את התועלת עבור הארגון.
- **ביצוע ניתוחי עומק של השימושים הארגוניים בענן:** בקרה שוטפת וניהול סיכונים פיננסיים של כלל הפרויקטים הארגוניים בענן והפקת תובנות ביחס לפעילות ולעדכון המלצות/הנחיות בהתאם.
- **ביצוע התאמות ואופטימיזציה בשירותים:** אופטימיזציה בשירותים ובאפליקציות על מנת להבטיח יעילות מרבית

לאורך זמן, ניצול מיטבי של משאבים והתאמתם לצרכים העסקיים בהתאם למודלי התמחור הרלוונטיים.

## 5.4 ניהול השינוי והיבטים ארגוניים

עומק הטרנספורמציה שמחולל הענן בשיטות העבודה והיקפה מחייבים שינוי בדרכי הפעולה של הממשלה לא רק בהיבט הטכנולוגי, אלא גם בשינוי התהליכים ודפוסי העבודה הקיימים ובמשאב ההון האנושי. לאור זאת, הממשלה תשקיע בתכנון המהלך על מנת לייצר יסודות יציבים, שיתמכו במעבר הממשלה לענן לאורך השנים, בהתאם לעקרונות פעולה לניהול השינוי לצורך הפעלה יעילה ומיטבית:

### 5.4.1 מיקוד ביצירת ערך עבור משרדי הממשלה

ניהול המעבר לענן יתבסס על תהליכי הטמעה שיטתיים ומהירים של שירותים סטנדרטיים לרוחב הממשלה, בהתבסס על איסוף צרכים, ניתוח של נתוני שימוש ומענה למשוב העולה מן השטח, תוך קידום תפיסה אג'ילית (Agile) ושיתוף פעולה שוטף עם צוותי היישום של הענן להתאמת מפת הדרכים למימוש.

**תועלות:**

- סנכרון בין התפיסה האסטרטגית לצוותי היישום בענן.
- הלימה בין התפתחות הפתרונות הטכנולוגיים בענן לבין הצרכים העסקיים ומידת הבשלות של משרדי הממשלה.
- שימוש אופטימלי ואפקטיבי במשאבים ובפתרונות הטכנולוגיים השונים בהתאם לדרישות ולצרכים השונים של המשתמשים.

### 5.4.2 תהליך עבודה משתף והגדרה של תהליכי שינוי במודל ההפעלה

המפתח להצלחה בשינוי האסטרטגי של מעבר הממשלה לענן הוא יצירת שיתוף פעולה של גורמי המטה השונים בין עצמם ובין משרדי הממשלה הפועלים בשטח. עיקרון זה מתווה אופן פעולה המכליל את השותפים, תוך היוועצות עם בעלי העניין השונים בתהליך השינוי, לרבות תכנון אסטרטגיית הענן, מדיניות השימוש בענן, הסטנדרטים שייושמו ותעדוף המהלכים. במסגרת עיקרון זה יתבצע מיפוי של בעלי העניין ובעלי התפקידים הרלוונטיים וכיצד יושפעו מהשינוי שחל במסגרת המעבר לענן, לרבות התאמת תפקידים והון אנושי נדרש, תחומי אחריות, כלים והכשרות נדרשים והתאמה לצורכיהם בעלי עניין שונים, טכנולוגיים ועסקיים.

**תועלות:**

- פירוק של הסילואים (silos) הקיימים תוך זיהוי חסמים ואתגרים בשלבים מוקדמים ויצירת שיתוף פעולה להסרתם.
- מתן ביטוי ליתרון היחסי של כל אחד מהגורמים השותפים.

יצירת שיתוף פעולה לטובת קידום של מהלכי ליבה ארוכי טווח.

### 5.4.3 שיתוף ידע מקצועי ושקיפות

בהמשך להקמת ה-CCoE, יש חשיבות לתכנון ולהקצאה של משאבים לטובת שיתוף הידע המקצועי הנצבר לקהלי היעד הרלוונטיים בכל תחום. האקו-סיסטם הממשלתי לענן יכלול הנגשת מידע מקצועי, הנחיות, כלים והכשרות לכלל הקהלים, טכניים ועסקיים כאחד. מינוף קהילות הידע הקיימות יאפשר שיקוף ושיתוף ניסיון מעשי העולה מן השטח.

**תועלות:**

שיתוף ידע על הצלחות, על אתגרים ועל דרכי התמודדות במעבר לענן, בדגש על אימוץ יישומים בענן המניבים ערך עסקי.

קידום של תפיסות ושיטות עבודה משותפות לכלל גורמי הממשלה.

יכולת של הפצת תבניות (טמפלטים) ובנייה של מאגר קוד מרכזי לשימוש המשרדים.

יצירה של רשת קשרים מקצועית, התומכת בשיתופי פעולה בין-משרדיים ובלמידת עמיתים.

### 5.4.4 התאמת ההון האנושי והממשלתי לעבודה בענן

מהפכת הענן יוצרת שינוי מהותי בעבודתם של צוותים טכנולוגיים, לרבות סט חדש של יכולות מקצועיות ושל תפקידים הנדרשים לצורך מימוש אפקטיבי של יתרונות הענן. כמתואר בפרק 2 למסמך זה, כיום מתמודדת הממשלה עם פער מיומנות משמעותי בכל הקשור בעולם הענן ועם משבר כולל בהון האנושי הטכנולוגי וביכולת לענות על צורכי המערכת.

על מנת לגשר על הפער בין המצב הקיים ליכולות הנדרשות, הממשלה תפעל באופן יזום להתאמה ולחיזוק של ההון האנושי הטכנולוגי והעסקי. לצורך כך, המדיניות תותאם לצרכים המשתנים, והממשלה תפעל בכמה צירים קריטיים להתאמת ההון האנושי לענן:

- יצירת תוכניות ייעודיות לפיתוח מקצועי של ההון האנושי הקיים.
- הגדרת תפקידים ייעודיים חדשים לענן.
- התאמת המבנה הארגוני במשרדי הממשלה, בדגש על אגפי טכנולוגיות דיגיטליות ומידע.
- קידום של ערוצי גיוס אפקטיביים.

**תועלות:**

שיפור יכולתה של הממשלה לממש את פוטנציאל המעבר לענן.

פיתוח ההון האנושי במקצועות טכנולוגיים מתקדמים, תוך יצירת הזדמנויות להתקדמות מקצועית ולצבירת ידע מעשי בתחום הענן.

צמצום הפער הטכנולוגי בין הממשלה למשק ושיפור האטרקטיביות של הממשלה כמעסיק.

הגדלת הפריון של ההון האנושי בשירות המדינה באמצעות גישה לכלים ולשיטות עבודה מתקדמות.

בהמשך לפרסום האסטרטגיה, הנחיות המדיניות למימושם של עקרונות ההפעלה בנושאים השונים המתוארים בפרק זה תפורסמנה במסגרת מסמכי הנחיה ייעודיים על ידי גורמי המקצוע המובילים בכל אחד מתחומי האחריות של ה-CCoE.

# 6 | ניהול סיכונים

## 6.1 מפת הסיכונים בענן

מעצם טבעו, ענן ציבורי חושף את הארגון לסיכונים מסוגים שונים מאלו הקיימים בתשתיות On Premises. סיכונים אלו נובעים, בין השאר, מהיותו של הענן הציבורי בעל פוטנציאל חשיפה לרשת האינטרנט, מהמיקום הגיאוגרפי של תשתיות הענן, מהדומיננטיות של ספקי הענן הגדולים ועוד. עם זאת, באופן כללי שימוש בענן ציבורי משפר את הגנות הסייבר ביחס לחלופות ה-IT הקיימות, כאשר הפלטפורמה מציעה את הטכנולוגיה החדישה ביותר, שמתעדכנת תדיר ומספקת את הכלים המתקדמים ביותר, תוך שדרוג מתמיד בהתאם להתפתחויות טכנולוגיות ולצורכי הלקוחות.

גיבוש מתודולוגיה של ניהול סיכונים ביחס לעבודת הממשלה בענן ייעשה בהתייחס לכמה קטגוריות, המצריכות התייחסות מעמיקה וייעודית:

### 6.1.1 סיכוני סייבר

סיכונים אלו נוגעים בעיקר למידע במערכות הממשלה ולרגולציה החלה עליו, וכוללים את סיכוני הסייבר המרכזיים, דוגמת פריצות לתשתיות הענן הציבורי, דליפה או אובדן מידע, אי-עמידה ברגולציה ובחוקי הגנת הפרטיות ועוד. בעוד שסיכונים אלו אינם ייחודיים לענן, במעבר לענן יש להם מורכבות ורגישות מיוחדת, שימוש בתשתיות משותפות וריבוי לקוחות (tenants).

### 6.1.2 סיכוני משילות וריבונות (Data Sovereignty)

פרויקט "נימבוס" ואסטרטגיית הענן הממשלתית נועדו בבסיסם להתמודד עם סוגיית המשילות של מערכות ומידע ממשלתי, וזאת באמצעות בניית המסגרת המשפטית והרגולטורית וכן שימוש בטכנולוגיה ליצירת מעטפת הגנת סייבר החלה עליהם. הסיכונים לשמירת הריבונות על המידע והתשתיות כוללים מגבלות משפטיות, שעלולות לסכן את רציפותם של שירותי הענן, חשיפה לצווים משפטיים בחו"ל, הנוגעים למערכות או למידע הממשלתי, היבטי רישוי ועוד. סיכונים אלו וההתייחסות אליהם במסגרת מכרז "נימבוס" מפורטים בסעיף 6.3 למסמך זה.

### 6.1.3 סיכוני תקציב

מודל התמחור של שירותים בענן, המבוסס על גישת pay-as-you-go, מייצר שינוי מחשבתי ותפעולי בניהול ההוצאה התקציבית על IT. שינוי זה טומן בחובו סיכונים כגון גידול בלתי צפוי או בלתי מתוכנן בעלויות הענן עקב אירועי קיצון,

הקצאה בלתי יעילה עקב חוסר ניסיון או מומחיות בעבודה עם תשתיות ענן וסיכוני עלות במעבר בין ספקים. סיכונים אלו יידונו וינוהלו במסגרת תפיסת ההפעלה לניהול תקציבי בענן - FinOps.

### 6.1.4 סיכוני טכנולוגיה

סיכונים אלו נוגעים לבשלות הטכנולוגית של משרדי הממשלה וליכולת להתאים את הטכנולוגיות השונות לצורכי הארגון. הם כוללים, בין היתר, אתגרי סטנדרטיזציה ותאימות בין סביבת ה-On Premises לסביבת הענן, תדירות שינויים גבוהה, גמישות מוגבלת בהתאמת הפלטפורמות (customization), תלות בתשתיות ובתצורת העבודה של ספק הענן, וכניסתן של טכנולוגיות חדשות, הדורשות אינטגרציה מורכבת ומיומנויות טכנולוגיות גבוהות.

### 6.1.5 סיכונים הקשורים לספקי שירותי הענן

סיכונים אלו נכונים לכל התקשרות עם ספק חיצוני, אך מידת ההסתמכות על ספקי שירותי הענן מחייבת התייחסות ייעודית למורכבות ולתלות הנוצרת מעצם השימוש בענן ציבורי. הסיכונים המרכזיים בקטגוריה זו הם "נעילת ספק" (Vendor lock-in) ופיתוח תלות-יתר בספקי הענן, ניצול לרעה של כוח שוק או ניגוד אינטרסים של הספק ביחס לממשלה, העשוי להשפיע על רציפותם או על איכותם של השירותים הניתנים לממשלה (לדוגמה, לחץ ציבורי כנגד מתן שירותים לממשלת ישראל). קטגוריה זו משיקה לסיכוני המשילות בשל ההיבטים המשפטיים והכלים שנעשה בהם שימוש כדי למתן את הסיכון.

### 6.1.6 סיכוני תפעול הענן

סיכוני תפעול מתייחסים בעיקר לרציפות שירותי הענן ולזמינותם, ליכולת להתאים את רמת השירות לצורכי הארגון ולאתגרי השליטה בזמינות המשאבים וביכולות ההתאוששות מאסון. עם זאת, ככלל, צמצום של סיכוני תפעול הוא אחד מיתרונותיה המובנים של תשתית ענן ביחס לתשתית On-Premises.

פרק זה מכיל עקרונות ליבה לניהול הסיכונים בענן, בדגש על אסטרטגיית הסייבר והיבטי המשילות. כלל קטגוריות הסיכונים תקבלנה מענה מפורט במסמכי המשך, במסגרת המדיניות הממשלתית הנגזרת מאסטרטגיית הענן, ובכלל זה תרחישים, שיטות להפחתת הסיכון (risk mitigation) ודרכי פעולה, אשר נועדו לוודא את היציבות ואת ההמשכיות העסקית של פעילות הממשלה.

## 6.2 עקרונות אסטרטגיית הסייבר הממשלתית בענן

מכרז "נימבוס" והחלטת הממשלה על אימוץ אסטרטגי של הענן מהווים קפיצת דרך משמעותית להוספת שירותים ממשלתיים מודרניים לאזרחי המדינה. בהיבטי סייבר והגנת מידע, תהליכי גיבוש האסטרטגיה, המדיניות ותפיסת ההגנה מלווים על ידי מערך הדיגיטל ועל ידי מערך הסייבר הלאומי.

מטרת-העל בהיבטי סייבר היא הבטחת הרציפות התפעולית של התשתיות הטכנולוגיות והמידע הממשלתי בענן, תוך הבטחת המשילות והריבונות, בין היתר באמצעות כלי הגנה בסייבר. הגדרת המסגרת לניהול הסיכונים בשימוש ממשלתי בענן ציבורי היא מרכיב משמעותי בבניית תהליך מעבר מוגן סייבר לענן ציבורי. ניהול הגנה מרכזי עם תפיסה הוליסטית, יישום בקרות סייבר להגנה על המידע, בקרה וניטור אחר פעילות חריגה במערכות ואופן השימוש בהן הם תנאים עיקריים להגנה על נכסי המדינה שבענן ציבורי.

ככלל, במעבר לענן ציבורי במסגרת פרויקט "נימבוס", ברירת המחדל היא אישור מעבר והקמה של מערכות בענן בהתאם לעקרון cloud first, למעט מקרי קצה. לצורך כך הוגדר מתווה "רמזור", המסייע בסיווג מידע ומערכות לצורך ההחלטה על מעבר לענן, כמפורט בסעיף 6.3.2.5.

### 6.2.1 עקרונות להגנת סייבר בענן

**6.2.1.1 ניהול סיכונים והערכת סיכוני סייבר בענן:** הממשלה תקיים תהליכי ניהול סיכונים רציפים בהיבטי אבטחת מידע וסייבר, שכוללים זיהוי, תיעוד והערכת איומי הסייבר באמצעות כלים תומכים כגון מחשבון סיכונים ייעודי אשר יסייע לזהות את רמת הסיכון והבקרה הנדרשת. זאת לצד בקרה רציפה על ידי שימוש במערכות אוטומטיות לבחינה של Cyber POSTURE, הפעלת תהליכים מנוהלים ומבוקרים, הטמעת בקרות לצמצום הסיכון למערכות לרמה המקובלת ובחירה בפתרונות התואמים את רמת הסיכון.

**6.2.1.2 סיווג המידע והמערכות:** עיקרון זה מתייחס לסיווג המידע והמערכות השונות במשרדים כשלב מקדים לקבלת החלטות הקשורות לשיקולי הגירה, בחירת השירות המתאים והפעלת מערכות ממשלתיות בענן. כדי לאפשר קבלת החלטות מושכלת ומבוססת לניהול סיכונים, תוגדר מדיניות לסיווג נתונים ומערכות מידע בכל מחזור שלבי החיים של המידע. המדיניות תכלול, בין היתר, את השיקולים והקריטריונים לסיווג המידע והמערכות לטובת מעבר לענן, בהתייחס גם לסיכונים המשפטיים ותוך מתן משקל מתאים לאותם סיכונים, כגון רגישות המידע בהיבטי פרטיות, היקף הרשומות, קריטיות התהליכים התפעוליים, תקופת הפעילות, סוג הסביבה במחזור החיים של המערכת (פיתוח, בדיקות או ייצור), מיקום פיזי של המידע, נזק פוטנציאלי ועוד.

**6.2.1.3 קווים מנחים, סטנדרטיזציה ודרישות סף:** כדי לאפשר עצמאות וחופש פעולה מפוקח למשרדי הממשלה בהקמה והגירה של מערכות מידע באופן עצמאי, תוך שמירה על רמת אבטחה נאותה, הממשלה החליטה לאמץ את תקני ה-ISO. מערכות ממשלתיות בענן ציבורי יעמדו בתקנים בין-לאומיים רלוונטיים. בנוסף, תוגדר במסגרת ה-CCoE מדיניות, קווים מנחים, best practices, אשר יכללו הנחיות, משאבים בני שיתוף, פלטפורמות, כלים ושיטות הפעלה למנגנוני משילות, בקרה, הגנה, ניטור ותגובה בענן, אשר לאורם יפעלו המשרדים.

**6.2.1.4 בקרות ואמצעי הגנת סייבר:** המידע הממשלתי המנוהל במשרדי הממשלה ויחידות הסמך עשוי לכלול מידע פרטי ורגיש על אנשים, על גופים ועל גורמים נוספים או על תהליכים ממשלתיים. לפיכך, בשימוש בענן ציבורי יוודאו משרדי הממשלה, כי המערכת מוקמת ופועלת בענן ציבורי תוך מימוש הגנות ובקרות לאבטחת מידע ומספקת את ההגנה הראויה למידע ולשימוש הנדרש לצורך ניהול מידע על פי סיווגו (ראו סעיף 6.2.1.2 לעיל). לצורך כך תנקוט הממשלה אמצעים טכנולוגיים ותהליכיים מתאימים בכל שלבי היישום בענן: בעת תכנון פתרונות טכנולוגיים (Security by Design), בתהליכים של הגירת מערכות לענן וביישום של פתרונות לאורך מחזור חייהם. הממשלה תממש תהליכי

בקרות לגילוי ולמניעה, הפועלות ברציפות ומבוססות אוטומציה, כך שיפעלו לזהות, להתריע ולמנוע סיכונים מיד עם היווצרות הפרצה או הסיכון. דרישות אלו ימומשו על ידי שימוש בכלים ובמוצרים חדשניים מותאמי ענן, בשיטות עבודה אוטומטיות ובשיתוף ידע ומשאבים ותהליכים בכל תחומי הגנת הסייבר והמשילות.

### 6.2.2 מימוש עקרונות של אסטרטגיית הגנת סייבר בענן

על מנת לממש את העקרונות הנמנים בסעיף 6.2.1, תשתית אירוח בענן לטובת הקמת שירותים ממשלתיים תתבסס על מרכיבי יסוד ועל תחומי פעילות למימוש סביבת ענן ממשלתית מאובטחת, התואמת את חזון הממשלה לענן ואת המטרות שהוגדרו עבורו. אסטרטגיית הגנת הסייבר הממשלתית בענן מבוססת על מודל בשלות, המתמקד בתחומי הפעילות הבאים:

**6.2.2.1 משילות של אבטחת מידע וסייבר בענן:** משילות ממשלתית בענן (Governance, Risk, Compliance - GRC) תאפשר החלת מדיניות וקווים מנחים על כלל המערכות והמשרדים, לרבות נראות מלאה של תהליכים, משאבים והמידע בענן לצורך ניהולו. תחומי המשילות האסטרטגיים הבאים לידי ביטוי במסמכי המדיניות לעבודת הממשלה בסביבת הענן מורכבים ממשילות סייבר (Governance), מניהול סיכוני סייבר (Risk Management) ומעמידה בתקנים בין-לאומיים להגנת סייבר בענן (Compliance).

**6.2.2.2 תפעול מערכות ותהליכי הגנת סייבר בענן:** לצורך עמידה ביעד המשילות של אבטחת סייבר בענן על הממשלה להחזיק ולהפעיל כוח אדם מיומן ובעל הכשרות מתאימות כדי לקיים את תהליכי התפעול להגנת הסייבר ולאבטחת מידע במערכות באופן מרכזי, תוך תמיכה בקיום משילות ובצמצום סיכונים. לצורך כך נדרשת תשתית תפעולית, הכוללת תהליכים, כלים ומשאבים משותפים. מרכיבי ה-SecOps העיקריים כוללים ניטור, תחקור, תגובה וטיפול באירועים, שימוש במידע מודיעיני וניהול חשיפות בתוכנה, זאת לצורך שמירה על יעילות, על שיתוף ושימור ידע ועל אחידות בשיטות הביצוע בממשלה, המנצלות את אספקתם עם יתרון הניהול המרכזי ברמה הממשלתית.

**6.2.2.3 אבטחת תהליכי פיתוח:** אבטחת תהליכי הפיתוח (SecDevOps) למערכות מידע לסביבות ענן תתבצע תוך מתן דגש על נושא שילוב האבטחה והגנת סייבר בתהליכי הפיתוח, מראשיתם, וכתיבת הקוד סביב תשתיות הענן ואבטחתן. תפיסה זו מחייבת שילוב מתודולוגיות, כלים, סטנדרטים ושיטות חדשניות ומותאמות לפיתוח בענן והעברת המערכות משלב הקוד לסביבות הבדיקה והייצור ללא התערבות ידנית, זאת תוך שילוב כלים לבדיקות אוטומטיות ותהליכים ממוכנים משלב התכנון (Plan) והפיתוח (Code) של המערכת ועד לשחרור הגרסה (Release) וההרצה (Run).

**6.2.2.4 ניהול זהויות ובקרת גישה:** הגדרת מודל ומדיניות לניהול משתמשים (אנושיים ותהליכיים) והנגשת תשתית רוחבית לניהול זהויות דיגיטליות למשרדי הממשלה, לצורך מידול זהויות והרשאות, בקרת תהליכי הגישה ואכיפת גישת ההזדהות. לצורך מתן אפשרות לשיתוף גישה למערכות מידע ממשלתיות בין משרדים, משילות בתחום הזהויות הינה נדבך אסטרטגי, המאפשר ניהול וניטור זהויות של תהליכים ושל עובדי ונותני שירותים במשרדי הממשלה, תוך ניתוח של סיכוני התנהגות להקטנת הסיכונים.

**6.2.2.5 הגנה על מידע ומערכות:** תחום זה מגדיר את הדרך שבה יש לממש בקרות והגנות ברובד של רכיבי התשתית בענן (Infrastructure) (מכונות וירטואליות, רשתות תקשורת, קונטיינרים ורכיבי וירטואליזציה) והחלה של שיטות,

סטנדרטים, קווים מנחים, הנחיות, כלים, מוצרים ותשתיות תומכות בתחום זה על כלל משרדי הממשלה לצורך יצירת סטנדרט תפעול והגנה אחיד בכל משרדי הממשלה. הממשלה תפעל למקסם שימוש במשאבים משותפים והפעלת אוטומציה ליישום ולהגנה של משאבי הענן ולמזער ביצוע תהליכים, שינויים והתאמות באופן ידני.

## 6.3 היבטים משפטיים בניהול סיכוני ענן

פרק זה סוקר את ההיבטים המשפטיים הרלוונטיים לניהול סיכונים בעולם הענן הציבורי, ובפרט בהתייחס לסיכונים אלו בתהליך מעבר הממשלה לענן במסגרת פרויקט נימבוס. כדי לקיים דיון בסיכונים המשפטיים בענן, יש להבין את אופי היחסים עם ספקי ענן ציבורי, את נקודות התורפה המשפטיות, ואת הכלים שמספק החוזה במסגרת פרויקט נימבוס.

הייחודיות הקיימת בניהול סיכוני ענן מתמקדת בהיבטים שונים של איבוד שליטה על המידע ועל המערכות התפעוליות, כאשר שימוש במחשוב ענן משמעותו הוצאת המערכות והמידע הממשלתי לתשתיות המופעלות על ידי ספק חיצוני והמשותפות, במידה מסוימת, לכלל לקוחותיו, כמתואר בסעיף 2.1 למסמך זה. נוסף על האמור, עולם הענן הוא ריכוזי ומתאפיין במיעוט שחקני ענן במשק העולמי. בהקשר זה, יש לציין במסגרת פרויקט "נימבוס" עומדים לרשות הממשלה שני ספקי ענן ציבורי מבין ארבעת הספקים המובילים בעולם, אשר עומדים בתנאים המיוחדים שהוגדרו במכרז "נימבוס", שמטרתם לתת מענה לסיכונים המשפטיים וההגנתיים המפורטים בפרק זה.

### 6.3.1 סוגי סיכונים משפטיים בענן[5]

בהיבטים משפטיים, ניתן להגדיר כמה גורמים עיקריים, המשפיעים על הסיכון לאיבוד שליטה במערכות או במידע:

- ספקי הענן וחלק מספקי השירותים הם תאגידי ענק גלובליים בעלי כוח והון רב.
- לספקי הענן מדיניות עצמאית גם בהיבטים "מסחריים", אבל גם בהיבטים של קביעת נורמות (רגולציה עצמית).
- ספקי הענן נתונים לרגולציה של מדינות שונות ולפניות של ערכאות מחוץ לישראל, באופן שעשוי להשפיע על מתן השירותים בישראל.

כמפורט להלן, חלק מהסיכונים נוגעים להתנגשות עם נורמות חוקיות של מדינות זרות, או לאינטרסים של ספקי ענן, כאשר מנגד ישנן במכרז הוראות במעמד נורמטיבי של חוזה. לאור האמור, לצורך התמודדות עם סיכונים נכללות בהתקשרות עם ספקי "נימבוס" הוראות הקבועות בחוזה, אשר יוצרות נורמות חוקיות בהתאם לדין בישראל (לדוגמה, סודיות), כאשר הפרה של נורמות אלו יכולה להוות עבירה פלילית בהתאם לדין הישראלי. בנוסף, הוגדר צורך לאכיפה של דרישות החוזה באמצעות בתי משפט בישראל, כאשר בהקשר זה החוזה קובע סמכות שיפוט לבתי משפט בישראל וברירת דין ישראלית.

1. **סיכונים הנובעים מאופי ספקיות הענן כתאגידי ענק גלובליים**

[5] יודגש, כי פרק זה לא מתמקד בסיכונים המסחריים הרגילים הקיימים בעת התקשרות עם ספקים, והדגש הוא על הסיכונים הייחודיים הקיימים בשימוש בענן ציבורי דווקא.

ספקיות הענן הן תאגידי ענק גלובליים, אשר המטה שלהן יושב בארה"ב (חברות אם), ויש להן חברות-בנות ברחבי העולם. חברות אלו מעסיקות מאות אלפי עובדים ברחבי העולם, ולפחות מאות עובדים בישראל. מבנה זה מאפשר לספקיות הענן לשנות בקלות יחסית את מבנה הבעלות של אופן אספקת שירותי הענן, להחליט על הפסקת פעילות מסוימת, או להחליט שלקוח מסוים מסב נזק ולהפסיק למכור לו שירותים.

### 2. סיכונים הנובעים ממדיניות עצמאית של ספקיות הענן

כחלק מהיותם תאגידי ענק, לספקי הענן יש מדיניות עצמאית ביחס לאופן אספקת שירותיהם ולאילו לקוחות השירותים נמכרים. הפרה של כללי השירות של ספקי הענן, או שינוי מדיניות של הספקים עלולים להביא להפסקת אספקת השירות. בהקשר זה יצוין, כי המדיניות של ספקי הענן עשויה להיות מושפעת מתפיסות ומעמדות פוליטיות שונות. כך, למשל, ידוע כי קיימת ביקורת ציבורית בין-לאומית על כך שספקיות הענן מעניקות שירות למדינת ישראל. ביקורת שכזו עשויה לייצר לחץ על ספקיות הענן לשנות את מדיניותן, ובנסיבות מסוימות עלולה להוות סיכון לרציפות העסקית באספקת השירותים לממשלה שיש להביאו בחשבון במסגרת ניהול הסיכונים.

### 3. חשיפה פוטנציאלית לתחולת דין זר ולפניות מצד ערכאות זרות

ספקי הענן הם תאגידים גלובליים, הנתונים לרגולציה של המדינות השונות שבהן הם פועלים. כמו כן, כתאגידים אמריקניים, חברות אלו נתונות לרגולציה מוגברת של ארה"ב. במסגרת זו, הרגולציה חוצה לעיתים גבולות של מדינות וחלה על ספקי הענן גם כאשר הם פועלים במסגרת של מדינה ריבונית אחרת (כדוגמת ה-Cloud Act). בנוסף, הספקיות חשופות לצווים מצד ערכאות זרות, כגון צו כנגד ספק שירותי ענן במסגרת מכרז הענן, שבמסגרתו נדרש הספק להימנע ממכירת שירות לאורגן של ממשלת ישראל, להגביל את השירות או למנוע את הגישה של משתמש מסוים לשירות; או צו לקבלת מידע או נתונים המצויים בידי ספק שירותי הענן במסגרת הליך פלילי או הליך אזרחי בין שני צדדים שלישיים.

## 6.3.2 עקרונות לניהול הסיכונים המשפטיים בענן

**6.3.2.1 שמירה על משילות וריבונות המידע והמערכות:** בהקשר זה, המונח "משילות וריבונות המידע" בהקשר למסמך זה מתייחס ליכולת של המדינה לשלוט במידע שלה ובכלל זאת שהמידע והתשתיות לא יהיו נתונים להפעלה של סמכויות שלא נקבעו על ידי המדינה, כגון חקיקה, נהלים או דינים שאינם ישראליים. על כן ככלל, המערכות הממשלתיות יוקמו ויתופעלו באזור הישראלי. בשלב הביניים יוכלו משרדי הממשלה להשתמש בענני "נימבוס" של הספקיות הזוכות ולצרוך שירותי ענן ציבורי ממרכזי ענן ספציפיים הנמצאים במדינות האיחוד האירופי, בהתאם לתנאי "נימבוס" בענני חו"ל, כאשר עם הקמת האזור הישראלי הקבוע יעבירו המשרדים את המערכות והמידע הנדרשים לכך לאזורי ענן במדינת ישראל.

**6.3.2.2 שימוש בכלים חוזיים:** חלק מהסיכונים שפורטו לעיל נוגעים להתנגשות עם נורמות חוקיות של מדינות זרות או עם אינטרסים של ספקי ענן. החוזה שנערך במסגרת פרויקט "נימבוס" קבע הוראות לצורך התמודדות עם הסיכונים השונים, ובפרט המשפטיים, אשר מטרתן לייצר, ככל האפשר, נורמות חוקיות בהתאם לדין בישראל ולאקלים המשפטי הישראלי לניהול כלל ההליכים שעשויים להיווצר במסגרת תקופת ההתקשרות. בין היתר, נקבע, כי: ההתקשרות תהא מול גוף ישראלי; סמכות שיפוט לבתי משפט בישראל וברירת דין ישראלית; ערבויות ואחריות אישית של נושאי משרה;

התקשרות מרכזית על פי תנאים שהוכתבו במכרז ולא על פי תנאים סטנדרטיים של ספקי הענן; ההתקשרות היא מול שני ספקים ענן שונים, תוך הפחתת הסיכון ל"נעילת ספק" (vendor lock-in).

**6.3.2.3 סיווג מידע ומערכות:** בדומה לעיקרון זה בניהול סיכוני סייבר, הממשלה תגדיר מדיניות משפטית מפורטת לשיקולים בהעברת מערכות ומידע לענן במסגרת פרויקט "נימבוס", בדגש על משמעויות השימוש בענן בחו"ל או בשטח ישראל (ראו סעיף 6.2.1.2 למסמך זה).

**6.3.2.4 גיבוש מדיניות משפטית מפורטת:** על אף הבקרות הרבות הקבועות בחוזה והשיפור הניכר מבחינת המצב המשפטי והיכולת להגן על המערכות והמידע הממשלתי, הרי שעדיין קיימת הסתברות מסוימת להתממשות הסיכונים שפורטו מעלה, ולפיכך יש צורך בקביעת מדיניות משפטית בעת המעבר הממשלתי לענן כחלק מהמדיניות הממשלתית הכללית לנושא. על מנת לאפשר למשרדים עבודה עצמאית לניהול המעבר לענן, ובפרט ניהול סיכונים פרטניים ככל שיהיו, יש לייצר מדיניות משפטית ייעודית לתחום הענן, תוך פיתוח הכלים, הידע והמיומנויות הנדרשות בקרב גורמי המקצוע. מדיניות זו תכלול, בין היתר, מיפוי, ניתוח ובחינת השפעתם של המקורות המשפטיים הרלוונטיים החלים על פעילות הממשלה בענן, ובכלל זה הסכמי "נימבוס", חקיקה ישראלית רלוונטית, דינים זרים, הסכמים בין-לאומיים וחקיקה ספציפית הנוגעת לענן.

**6.3.2.5 כלים תומכי החלטה:** המדיניות המשפטית תתורגם להנחיות אופרטיביות על מנת לסייע למשרדים לקבל החלטות מושכלות בבואם לבחון העלאה של מידע או מערכת לענן. בכלל זה ייקבע מתווה "רמזור", שמטרתו לייצר מדרג של רגישות המערכת והמידע למול הסיכונים הפוטנציאליים והסיכוי להתממשותם, במטרה לסייע בהכרעה באילו תנאים ניתן להשתמש בענן בארץ ובחו"ל (או בשילוב בין כמה אזורים בהתאם לצורך ספציפי), או במקרי קיצון האם נכון לעלות מערכת לענן ציבורי. מתווה זה יאפשר למשרדים ליישם את המדיניות ולקבל החלטות בקלות וביעילות בבואם לשקול את היתרונות והחסרונות של בחירת פתרון זה או אחר לפני העלאת מידע או מערכת לענן. בטווח הארוך, מדיניות זו תסתייע בכלי טכנולוגי תומך-החלטה, אשר יסייע למשרדים לתרגם את עקרונות המדיניות וההנחיות האופרטיביות להנחיות ביצוע ועל מנת לסייע בניהול הסיכונים הכרוכים בהעלאת מידע ומערכות לענן.

**6.3.2.6 פיתוח מומחיות, מיומנויות וידע משפטי מקצועי לעולם הענן:** לרשות המשרדים יועמד מרכז ידע ומידע לגבי היבטים המשפטיים והרגולטוריים הרלוונטיים לענן בכלל ולענן במסגרת פרויקט "נימבוס" בפרט הן כבסיס לגיבוש המדיניות המשפטית–ממשלתית באופן מושכל, אפקטיבי ודינמי, והן כגורם מומחה, שהמשרדים יוכלו להיוועץ בו בתחום הענן אף בנושאים שלא הוסדרו במסגרת גיבוש המדיניות המפורטת.

מעטפת ההגנה החוזית במסגרת פרויקט "נימבוס" מייצרת סט רחב של כלים, שנועדו לתת מענה לסיכונים משפטיים ולשאלת הריבונות של מידע ומערכות ממשלתיות. מעטפת זו, בצירוף מעקב ובקרה על אכיפת ההוראות ותוך יישום של המדיניות המשפטית שתיקבע, בסיוע ההנחיות האופרטיביות והיוועצות בהתאם לצורך עם מוקד הידע, מהווים מענה משפטי הוליסטי להתמודדות עם הסיכונים שתוארו ויאפשרו תהליך ממשלתי אפקטיבי במעבר לענן במסגרת פרויקט "נימבוס".

# 7 | מדדי הצלחה למעבר הממשלה לענן

מטרת פרק זה היא לתרגם את אסטרטגיית הענן הממשלתית, המוגדרת בפרקים הקודמים של מסמך זה, לכדי פרמטרים מדידים, שישקפו את התקדמות הממשלה בתהליך המעבר לענן, במטרה להוות מצפן למדידה ארוכת-טווח של אימוץ הענן בממשלה בראייה רוחבית, להבטיח את מימוש היעדים שנקבעו ולוודא שהתהליך עצמו מתבצע באופן אפקטיבי. תהליך המדידה נועד לאזן בין הראייה ארוכת הטווח לבין ביצוע משימות קצרות טווח, כך שתתאפשר בקרה על התקדמות הפרויקט והצלחתו, ובמידה שאופן הפעולה לא מוביל לתוצאות הרצויות לעדכן את תכנון העבודה.

על מנת לתמוך בפעילות הנרחבת והמורכבת של הענן, יוגדר מערך מדידה מפורט במסגרת תוכניות העבודה שייגזרו מאסטרטגיית הענן בכל אחד מהיבטי התפעול - טכנולוגיה, פיננסים ושינוי ארגוני. המסגרת המוצעת בפרק זה משקפת את המדדים המרכזיים שעליהם יתבסס מערך המדידה ואת המטריקות האפשריות לביצועה, בהתבסס על עבודת בנצ'מארק בין-לאומי ועל הסטנדרט המקובל בעולם למדידת פעילות של ארגונים בענן.

הגדרת המדדים מבוססת לא רק על היעדים האסטרטגיים, אלא גם על מידת הבשלות הנוכחית והעתידית של הממשלה ביחס לענן ועל הנתונים הזמינים על פעילות הממשלה בתחום, כאשר עבור חלק מהמדדים נדרש, ראשית, לייצר קו בסיס למדידה עתידית, וחלקם יימדדו בשלבים מאוחרים יותר לאחר התפתחות פעילות הענן בממשלה והתבססותה. איסוף הנתונים יתבצע באמצעות ניטור וניתוח לוגים טכניים על פעילות הענן, מדידה מבוססת סקרים ודיווח עצמי ומעקב במסגרת תהליכי המטה והמערכות התומכות בהן. ככלל, יינתן דגש למדידת שביעות הרצון של משתמשי הקצה בפרמטרים השונים של פעילות הענן, כגון שיפור השירותים, מגוון הכלים והמוצרים הזמינים לממשלה ועוד.

הטבלה שלהלן מתארת את מדדי ההצלחה המרכזיים **ודוגמאות לאינדיקטורים** רלוונטיים למדידתם:[6]

| מטרה | יעדים | מטריקה לדוגמה |
| --- | --- | --- |
| ביצוע קפיצת מדרגה ביכולותיה הטכנולוגיות של הממשלה | 1. הרחבת היקף השימוש הממשלתי בענן<br>2. ניצול אופטימלי של יכולות הענן<br>3. אימוץ והתנסות בטכנולוגיות חדשות. | - מספר מערכות שעלו לענן<br>- מספר מערכות שעברו מודרניזציה בתהליך המעבר לענן<br>- חשבונות משתמשים פעילים<br>- כמות אחסון בענן<br>- מספר תהליכי pipeline ci/cd אוטומטיים שהוגדרו<br>- היקפי השימוש ברובד 5 של מכרז "נימבוס"<br>- מספר שירותים ומוצרים הזמינים בענן עבור משרדי הממשלה<br>- מדידת שביעות רצון מהשירותים הזמינים לממשלה בענן* |
| שיפור השירותים והמוצרים הדיגיטליים לציבור (אזרחים ועסקים) | 1. קיצור זמני פיתוח של שירותים חדשים (Time to Market) | - כמות שירותי API חשופים בענן<br>- היקף השימוש בשירותי API |
| | 2. שיפור איכות ועדכניות המוצרים הדיגיטליים שהממשלה מספקת | - שביעות רצון משירותים דיגיטליים - ציבור ומשרדי הממשלה* |
| | 3. שיפור הגמישות והמדרגיות (Scalability) של הממשלה במענה לצרכים משתנים | - שיעור זמינות המערכות (להבדיל משיעור זמינות הענן)<br>- שיעור המערכות שהוגדר להן autoscale מבין כלל סוגי המערכות שבהן נדרש השימוש בכך |

[6] מדדים המסומנים ב-* הם מדדים עתידיים, התלויים בבגרות השימוש בענן בממשלה.

| מטרה | יעדים | מטריקה לדוגמה |
|---|---|---|
| שיפור האפקטיביות וייעול ההוצאה הממשלתית בתחום הטכנולוגי | 1. שיפור תהליכי הניהול הפיננסי בממשלה בתחום ה-IT | - שיעור הצמצום בהוצאה על תשתיות On Premises<br>- שיעור תקצוב הענן מתוך כלל תקציב לרכש IT<br>- רמת דיוק התחזיות התקציביות ביחס להוצאה לפועל |
| | 2. איגום משאבים בענן - שימוש בשירותים משותפים בענן ושימוש חוזר (reuse) במשאבים טכנולוגיים | - היקף השימוש בשירותים רוחביים מתוך כלל השימוש בענן<br>- היקף השימוש החוזר בתבניות ממשלתיות בענן<br>- היקף השימוש החוזר בקוד ממשלתי<br>- היקף השימוש החוזר בנתונים ממשלתיים<br>- היקף השימוש ביכולות רוחביות וכלים משותפים מתוך כלל השימוש בענן |
| הבטחת הריבונות וההגנה על התשתיות הטכנולוגיות והמידע הממשלתי | 1. חיזוק המשילות בתחומי הטכנולוגיה וההגנה בסייבר[7]<br>2. יצירה והגדרה של מסגרת מדיניות, סיווג מערכות ומידע, ניהול סיכונים וקווים מנחים לשימוש ממשלתי בענן ציבורי.<br>3. קידום השימוש בתשתית ענן ציבורי מוגנת סייבר ואיכותית באזור ישראלי. | - היקף המערכות המנוטרות מתוך המערכות בענן<br>- היקף התראות סייבר שאותרו וטופלו באמצעות אוטומציה בענן<br>- שיעור המשרדים המחוברים לשיתוף של policies בענן מתוך כלל המשרדים<br>- היקפי השימוש בכלי אבטחה ייעודיים לענן |

[7] חיזוק המשילות בתחומי הטכנולוגיה וההגנה בסייבר תעשה, בין השאר, באמצעות: שיפור יכולת הניטור המרכזי על פי מדיניות אחודה, לצורך גיבוש תמונת מצב רוחבית של כלל המגזר הממשלתי ושיפור יכולת היישום של מדיניות אבטחת מידע מרכזית ואפקטיבית, הממוקדת באתגרים העומדים בפני הממשלה.

| מטרה | יעדים | מטריקה לדוגמה |
|---|---|---|
| חיזוק היכולות המקצועיות של הממשלה | 4. הקטנת פערי המיומנויות הטכנולוגיות של ההון האנושי בשירות המדינה בעולמות הענן | - שיעור ההון האנושי שהשלים הכשרות ענן מתוך כלל ההון האנושי הרלוונטי<br>- שיעור ממוצע של עובדי ונותני השירותים באגפי מערכות המידע שתפקידם לתת מענה בענן מתוך סך העובדים ונותני השירותים באגף<br>- שיעור איוש משרות ייעודיות לענן* |
| | 5. קידום השימוש בנתונים במשרדי הממשלה | - היקף השימוש ביישומים ממוקדי דאטה[8], כולל ביישומי SaaS (מספר קריאות, רישיונות)<br>- מספר מאגרי המידע החדשים שהוקמו בענן |
| | 6. שיפור הנגישות של יחידות מקצועיות לכלים דיגיטליים מתקדמים | - שביעות רצון של יחידות מקצועיות מהמוצרים והשירותים העומדים לרשותן |

* כללי: מטריקה רוחבית נוספת שתיבחן - שיעור הצמצום בהוצאה על תשתיות On Premises.

[8] יישומים ממוקדי דאטה הם יישומים, שהצורך העסקי המרכזי שהוגדר עבורם הוא שימוש בנתונים, בדגש על יישומי אנליטיקה.

# 8 | יוזמות אסטרטגיות וצעדים להמשך

אסטרטגיית הענן המובאת במסמך זה נועדה להתוות דרך ולייצר עבור הממשלה יכולת לתכנן בראייה רוחבית את ההיבטים האופרטיביים של המעבר לענן. בנקודת זמן זו, יותר משנתיים אחרי ייזום פרויקט "נימבוס", פעילויות תשתית רבות לאימוץ הענן כבר מצויות בהקמה ובביצוע כחלק מהכנת השטח ומגיבוש המדיניות הממשלתית לתהליך המעבר. פרק זה משקף את היוזמות האסטרטגיות, הקיימות והעתידיות, המצויות בליבת הפרויקט נכון למועד פרסום מסמך זה.

## 8.1 מדיניות

במסגרת רובד 2 של פרויקט "נימבוס" החלה הקמת ה-CCoE בשיתוף גורמים רבים מתוך הממשלה. במסגרת זו, הממשלה פועלת לייצר מדיניות מוסדרת, אשר תשרת את המשרדים כבר מהשלבים הראשונים של אימוץ הענן. נכון להיום, פורסמה הנחיה להגירת מערכות לענן, כאשר בטווח הקרוב, לצד מסמך אסטרטגיה זה, מתוכנן פרסומה של מדיניות משלימה בכמה תחומי ליבה: מודל ההפעלה לענן, ניהול סיכוני סייבר, רגולציה וציות (GRC), מודל תפעול ענן, רגולציה משפטית וסכמה לסיווג דאטה.

## 8.2 טכנולוגיה

בהתאם לעיקרון ההפעלה של ניהול מרכזי, תוך שמירה על עצמאות תפעולית, הממשלה השלימה הקמת תשתית ראשונית למעבר המשרדים לענן באמצעות שירות מרכזי של אזור הנחיתה הממשלתי בענן. תשתית זו תורחב בהדרגה על פי תכנית סדורה, תוך עדכון ושיפור מתמיד, במטרה לתת מענה מלא לצרכים השונים והמורכבים הנובעים מניהול תצורה מרובת-עננים. יכולות אלו יאפשרו לממשלה התקדמות טכנולוגית באמצעות אוטומציה של תהליכים, ניטור עבודה ושירותים בענן ומימוש יכולות ניהול מתקדמות. במקביל, משרדי הממשלה החלו בתהליך סדור של מיפוי מערכות ותהליכים רלוונטיים למעבר לענן, בהתאם למדיניות ההגירה (מיגרציה) לענן שפורסמה במסגרת ה-CCoE, על ידי מערך הדיגיטל הלאומי.

## 8.3 תקציב ופיננסים

- בהתאם להחלטת ממשלה מס' 231 בדבר קידום המעבר הממשלתי לענן ציבורי, על מנת להאיץ את מעבר משרדי הממשלה לענן ולתמרץ פעילות זו, הוקמה קרן ייעודית בגובה כ-200 מיליון ש"ח.
- המעבר לענן מייצר שינוי משמעותי לא רק בהיבטים טכנולוגיים, אלא גם בשיטות ומנגנוני הביצוע התקציבי, לדוגמה שיטת pay-as-you-go, תשלום על פי צריכה ועוד. על מנת לתת לכך מענה, הממשלה בהובלת החשב הכללי באוצר ובתיאום עם ה-CCoE, החלה לגבש תפיסת הפעלה לניהול הביצוע התקציבי וה-billing בענן, אשר ממנה ייגזרו התהליכים התפעוליים לניהול פיננסי בענן (FinOps).

## 8.4 רכש

נכון להיום, הושלמו התהליכים המכרזיים עבור הרבדים הראשונים של פרויקט "נימבוס", המאפשרים כבר עתה לתכנן ולבצע את המעבר באמצעות תשתיות ספקיות הענן ורכש תפוקות של ספקים מומחים. לקראת העמדת תשתיות ענן ציבורי בשטח על ידי הספקיות הזוכות, הגופים השותפים לאסטרטגיית הענן יפעלו להשלמת הרבדים הנוספים, בדגש על יצירת מנגנוני התקשרות לרכישת מוצרים וכלים מתקדמים על גבי תשתיות אלו.

## 8.5 הון אנושי ושינוי ארגוני

כחלק אינטגרלי מתהליך ניהול השינוי, ובהתבסס על ההתקשרות עם ספקיות הענן ברובד 1 של פרויקט "נימבוס", הושלמה בנייה של תוכנית הכשרות נרחבת לפיתוח מיומנויות נדרשות לענן עבור עובדי המדינה ונותני שירותי המחשוב בממשלה, הכוללת הכשרות פרונטליות ומקוונות בתחומי ארכיטקטורה, סייבר, דאטה, תפעול ענן ועוד. במקביל נעשית עבודת מטה מעמיקה להתאמת ערוצי מיקור חוץ לטובת יכולת גיוס תחרותית של כוח אדם ייעודי לענן עבור משרדי הממשלה, כאשר בטווח הארוך מתוכננת הסדרת תפקידי ליבה בתחום הענן בממשלה והתאמת המבנה הארגוני לשינוי.

יוזמות אלו משקפות את המאמץ ואת המשאבים האדירים המושקעים בהצלחת המעבר של הממשלה לענן. השקעה זו מתחברת להשקעות הממשלה בעשור האחרון בטרנספורמציה דיגיטלית ובחיזוק יכולותיה הטכנולוגיות. מבחינה זו, מעבר הממשלה לענן מהווה שינוי טקטוני בדפוסים ובמנגנוני הפעולה וביכולתה לרתום טכנולוגיה לטובת שיפור השירות לציבור וחיזוק האפקטיביות, תוך ביצוע "חריש עמוק" ביכולות ובמערכות הקיימות. רוחב היריעה ומורכבות נושא הענן, ובפרט מעבר הממשלה לענן ציבורי, מחייבים תפיסת הפעלה, המבוססת על שיתוף פעולה מקצועי עם כלל בעלי העניין והשותפים כתנאי הכרחי להצלחת המהלך.

אסטרטגיית הענן הממשלתית, המתוארת במסמך זה, מניחה לפתחה של הממשלה הזדמנות לצמצם עוד יותר את הפערים הקיימים, ובכך לחזק את החיבור בין הטכנולוגיה לצרכים המקצועיים והעסקיים ולבצע את קפיצת המדרגה הנדרשת כדי לממש את יעדיה.

# נספח א | מילון מונחים

| | |
|---|---|
| Auto Scale | הגדלה והקטנה אוטומטית של המשאבים הנצרכים בהתאם לשינויים בשימוש ובביקוש ועל מנת לחסוך בעלויות בעת זמני שפל בביקוש |
| AWS | Amazon Web Services - פלטפורמת שירותי אינטרנט בתשתית בענן המסופקת ע"י חברת Amazon. |
| AWS Availability Zones | מיקומים שונים בתוך אזור AWS המתוכננים להיות מבודדים מתקלות באזורי זמינות אחרים. הם מספקים קישוריות רשת עם שיהוי (latency) נמוך לאזורי זמינות אחרים באותו אזור AWS. |
| CapEx | CapEX, או Capital Expenditures הם משאבים אותם הארגון משקיע ברכישה, שדרוג וניהול של משאבים פיסיקליים, כמו: מבנים, טכנולוגיות וציוד, הוצאות אלו משמשות לטווח ארוך, לרוב בעבור הוצאות הארגון על תפעול תשתיות On Premises, כגון חוות שרתים. |
| CI/CD pipeline | Continuous Integration/Continuous Delivery. שיטת עבודה אג'ילית המתמקדת בתהליכי הפצת תוכנה באופן אמין ובתדירות גבוהה. מתודולוגיה זו מתאפיינת בעבודה איטרטיבית (לעומת לינארית בעבר), אשר מאפשרת לצוותי הפיתוח לכתוב קוד, לשלב אותו במערכת, לבדוק אותו, לספק גרסאות ושינויים בשיתוף פעולה בין צוותי עבודה שונים. |
| Cloud Act | החוק האמריקאי החל על נתונים אלקטרוניים בשירותי ענן |
| Cloud first | גישה לפיה על הארגון לבחון כברירת מחדל פתרונות ענן בעת פיתוח תהליכים חדשים או התאמת תהליכים טכנולוגיים ישנים |
| Data Center (DC) | Data Center - מרכז הנתונים. הכוונה לתשתית וירטואלית או פיזית המשמשת את הארגון לאחסון ולתחזוקה של תשתית טכנולוגיית מידע. |
| DevOps | קיצור של פיתוח (Development) ותפעול (Operations). שילוב של משימות המבוצעות על-ידי צוותי פיתוח יישומים וצוותי תפעול מערכות של ארגון מסוים. שיטת פיתוח התוכנה של DevOps שמה דגש על שיתוף פעולה, תקשורת ואינטגרציה בין מפתחים ואנשי IT אחרים, במטרה לייעל את פיתוח התוכנה ואת הבטחת האיכות. |
| DevSecOps | Operations Development Security - יכולות אבטחה מתקדמות באמצעות כלים המשולבים בתוך תהליכי האוטומציה המנהלת את מחזור חיי התוכנה |
| Disaster Recovery (DR) | התאוששות מאסון. מכלול הנהלים והשיטות בהם ישתמש הארגון להחזיר את חוות השרתים שלו לפעילות מלאה לאחר ארוע אסון (לדוג' שחזור נתונים שאבדו) |

| | |
|---|---|
| FinOps | שילוב של המילים Finance ו DevOps. מושג זה מתאר את שיטות ניהול הOpex של הארגון בהתמקדות בהוצאות הקשורות לענן. מטרת שיטה זו היא לאפשר לצוותים השונים בארגון (עסקי, כלכלי וטכנולוגי) ניהול ושיפור העלויות הכלכליות בשימוש בשירותי הענן |
| GCP | Google Cloud Platform - פלטפורמת שירותי אינטרנט בתשתית בענן המסופקת ע"י חברת Google. |
| GCP Zone | מיקומים שונים בתוך אזור GCP המתוכננים להיות מבודדים מתקלות באזורי זמינות אחרים. הם מספקים קישוריות רשת עם שיהוי (latency) נמוך לאזורי זמינות אחרים באותו אזור GCP. |
| IaaS | Service Infrastructure as a - תשתית כשירות. מאפשר לארגון יכולות ניהול ופריסת משאבי מחשבון (אחסון, שרתים, רשתות, מערכות הפעלה וכו') בסיסיים. הארגון אינו מנהל או שולט בתשתית הענן המפיזית, אלא משתמש ביכולות אותן מחצין ספק הענן |
| IAM | Management Identity and Access - ניהול זהויות וגישה. הגדרה וניהול של התפקידים והרשאות הגישה של ישויות רשת בודדות (משתמשים והתקנים) למגוון יישומי ענן ויישומים מקומיים. |
| IOT (internet of things) | IOT ("האינטרנט של הדברים") הוא רשת שבה נקודות הקצה אינן משתמשי קצה אנושיים אלא חפצים פיזיים ("דברים"), המשובצים בחיישנים ובתוכנה, אשר מאפשרים תקשורת בין החפצים ויכולות איסוף וניתוח מידע, האינטרנט של הדברים כולל בין השאר את תחומי "הבית החכם", "העיר החכמה"', מכשור לביש, תעשייה חכמה, תחבורה חכמה (כגון מכוניות אוטונומיות וכבישים חכמים), רפואה חכמה ועוד |
| Landing Zone | סביבה מוגדרת עם מערך סטנדרטי של תשתית ענן מאובטחת, כללי מדיניות, שיטות עבודה מומלצות, הנחיות ושירותים מנוהלים באופן מרכזי תחת חשבון ראשי אחד (Root). אזורי נחיתה מספקים סביבה מוגדרת מראש המוקמת כקוד עבור ספקי ענן שונים כגון Google Cloud ו- AWS. אזורי נחיתה הם מבנה בעל תפיסה קונספטואלית אחידה בין ספקי הענן, הכולל שירותים משותפים וחשבונות של ארגוני-משנה בכל אחד מספקי הענן, אשר מאפשרים לממש את אמצעי ההגנה הארגוניים ולהקצות שירותים משותפים ולעדכן "מדיניות-על" (Policy). |
| Lift-and-Optimize | מעבר מדורג של תהליכי עבודה לענן כאשר בכל שלב מתבצעת אופטימיזציה של השימוש של המשאבים בענן ו "כיבוי" של התהליך שעבר מיגרציה עד שכל המערכת עובדת ופועלת בסביבה החדשה בענן. תפיסה זו נועדה למקסם את השימוש במשאבים וברישיונות על מנת להשיג רווח אמיתי ושיפור בעת מעבר מערכות לענן. |
| Lift-and-Shift | העברת אפליקציה או פעילות מסביבה אחת לאחרת מבלי לעצב מחדש את האפליקציה, זרימת העבודה או הארכיטקטורה של פריסת האפליקציה ע"ג משאבי המחשב בעת העברתה משרתים פיזיים או וירטואליים הפועלים בחצרי הלקוח לשרתים הפועלים בענן. |
| Machine Learning | למידת מכונה היא תת-תחום של בינה מלאכותית, אשר מגדירה באופן כללי את היכולת של מכונה לחקות התנהגות אנושית אינטיליגנטית. מערכות בינה מלאכותית משמשות לביצוע משימות מורכבות באופן הדומה לצורה בה בני אדם פותרים בעיות. |
| Marketplace | פלטפורמה לרכישת שירותי ענן המספקת ללקוחות גישה ליישומי תוכנה ושירותים המוצעים על ידי הספק עצמו או ספקים אחרים (צד ג'). |

| | |
|---|---|
| Multiple-Cloud | מודל של מחשוב ענן שבו ארגון משתמש בשילוב של מספר עננים, כגון: שני עננים ציבוריים או יותר, שני עננים פרטיים או יותר, או שילוב של עננים ציבוריים ופרטיים כדי להפיץ יישומים ושירותים. פתרון התואם לתפיסת ה- Multi-cloud הוא פתרון המחיל תפיסה קונספטואלית אחידה בין ספקי הענן |
| OLA | Operational Level Agreement – הסכם רמה תפעולית. מסמך המציין במפורש את התפקידים, האחריות, הפעולות, התהליכים והמדיניות הרלוונטיים, כדי שספק השירות יוכל לעמוד בהסכם רמת שירות מסוים. |
| On Premise | תוכנה או תשתית המופעלת על-גבי חומרה המצויה ברשותו של האדם או הארגון שמשתמשים בתוכנה או בתשתית. |
| OPEX | Operational Expenses – הוצאות תפעול. הן ההוצאות אותן הארגון מבצע באופן שוטף כחלק מפעילותו ומתאפיינות בתנודיות בהשוואה להוצאת CapEX: הוצאות שכר, צריכת משאבים, שיווק וכו'. |
| PaaS | Platform as a Service - פלטפורמה כשירות.מאפשר לארגון לספק, להפעיל ולנהל חבילות הכוללות פלטפורמות מחשוב (שרתים, אחסון, תקשורת) וישומים, ללא המורכבות בתחזוקה של תשתיות פיזיות. הדבר מאפשר למפתחים לייצר חבילות שלמות המכילות את כל המרכיבים להפעלת היישומים שלהם. |
| Rehost | אירוח מחדש הוא מעבר של שירותי תשתית כגון רשת, מחשוב ואחסון מארוח מקומי לארוח תחת תשית ספק שירותי ענן. בשיטה זו מעבירים את שירותי הארגון כמעט ללא תכנון מחדש, ובך הארגון ממשיך לעבוד בתצורה המוכרת לו ומקבל את היכולות הבסיסיות ביותר של הענן כמו סקיילביליות |
| SaaS | Software as a Service – תוכנה כשירות. מאפשר לארגון יכולות החצנת יישומי תוכנה הניתנים כשירותים הזמינים לצרכן על פי דרישה, ספקי הענן מארחים ומנהלים את האפליקציה והתשתית הבסיסית שלה. |
| Scale Up & Down | Scale Down - הקטנת כמות הנתונים המעובדת או המשאבים הדרושים לביצוע העיבוד,Scale up - הגדלת משאבי המחשוב , באמצעות עיבוד מקביל וטכנולוגיות זיכרון/אחסון מהירות יותר. |
| Silo (סילו) | מערכות אשר אינן מתקשרות עם מערכות אחרות (העברת מידע, החצנת מידע וכו'), מערכות סגורות אלה מקשות על הארגון ביצירת שפה משותפת, אמת אחת וקבלת החלטות מבוססות מידע בארגון. |
| SLA | Service Level Agreement - הסכם רמת שירות. רמת השירות המוגדרת המצופה מספק מסוים; מפרטת את המדדים שלפיהם השירות נמדד, כמו גם פיצויים או קנסות למקרה שרמות השירות המוסכמות לא יושגו. |
| Tagging (תיוג) | תהליך שבו משתמשים יכולים להוסיף מטא נתונים (Tags) תיאוריים לתשתית הענן שלהם. תג מורכב משני חלקים: מפתח וערך לזיהוי המשאב בענן. |
| Tenant | חשבון המוגדר בסביבת ענן משותפת. ענן מרובה חשבונות הוא ארכיטקטורת מחשוב ענן המאפשרת ללקוחות לשתף משאבי מחשוב בענן ציבורי או פרטי. הנתונים של כל חשבון מבודדים ונשארים בלתי נראים לחשבונות אחרים. |
| Virtual | רשת וירטואלית פרטית המהווה פתרון להעברה מאובטחת של מידע על גבי האינטרנט באופן מוצפן |

| | |
|---|---|
| Private Networks (VPN) | מקצה לקצה כך שהמידע איננו נגיש לגורם כלשהו מלבד בשתי נקודות הקצה. |
| אזור (Region) | שטח גיאוגרפי מוגדר, הכולל מדינה (Country) אחת, חלק ממדינה אחת או ישות על-מדינתית מוגדרת (כדוגמת "האיחוד האירופי"), אשר כולל "מתחם" אחד לפחות ממנו מסופקים שירותי ענן ללקוחות על ידי ספק שירותי ענן. |
| הגירה לענן, מיגרציה (Migration) | התהליך שבו כל/חלק מהנתונים, היישומים והשירותים מועברים מהתשתית המקומית לענן. |
| התאוששות מאסון | תחום תכנון האבטחה העוסק בהגנה על ארגון מפני ההשפעות של אסונות גדולים שמשמידים חלק מהמשאבים שלו או את כל המשאבים שלו, לרבות רשומות נתונים, ציוד IT והמרחב הפיזי של הארגון. תוכנית שחזור נתונים ממפה את הדרך המהירה והיעילה ביותר שבה ניתן לחדש את העבודה לאחר אסון. |
| מדיניות בענן (policy) | מדיניות ענן היא הקווים המנחים לפיהם חברות פועלות בענן, המתורגמים ליישום טכנולוגי של המדיניות באמצעות כללים אוטומטיים. מדיניות הענן מיושמת לעתים קרובות על מנת להבטיח את השלמות והפרטיות של מידע בבעלות החברה, יכולה לשמש גם לניהול פיננסי, אופטימיזציית עלויות, ניהול ביצועים ואבטחת רשת. |
| מדרגיות, סקיילביליות (Scalability) | מונח המשמש כדי להתייחס ליכולת של מערכת להסתגל לשינויים בביקוש של יישומים על-ידי הקצאה וביטול הקצאה של משאבים משותפים, כך שהמשאבים המוקצים יתאימו לביקוש הנוכחי בצורה הטובה ביותר. |
| מחשב וירטואלי, מכונה וירטואלית | מחשב מבוסס תוכנה (ללא חומרה) המריץ מערכת הפעלה או סביבת יישום, בדיוק כפי שחומרה פיזית הייתה עושה. |
| ניהול זמינות | תהליך המבטיח שרמת זמינות שירותי הענן המסופקים תואמת לצרכים המוסכמים של הארגון - הנוכחיים והעתידיים. תהליך זה כרוך ביצירה ותחזוקה של תוכנית זמינות מתאימה ועדכנית, המשקפת את הצרכים הנוכחיים והעתידיים, והמבטיחה שהעסק מבין את ההשלכות הפיננסיות של שינויים ברמת זמינות השירות. |
| נעילת ספק (Vendor lock-in) | מצב שבו לקוח המשתמש במוצר או שירות אינו יכול לעבור בקלות למוצר או שירות של מתחרה, בדרך כלל כתוצאה של טכנולוגיות קנייניות שאינן תואמות את אלו של המתחרים. |
| ספק שירותי ענן (CSP) | Cloud Service Provider - ספק שירותי ענן. לפי תקן ISO/IEC, ספק שירותי ענן הוא גורם שהופך שירותי ענן לזמינים. ספק שירותי הענן מתמקד בפעילויות הנחוצות למתן שירות ענן ותחזוקתו, ובפעילויות שנדרשות כדי להבטיח את אספקתו ללקוח שירותי הענן. |

| | |
|---|---|
| ענן היברידי | שימוש משולב של תשתית ענן פרטית וציבורית. גישת ענן היברידי כוללת שימוש בכלי ניהול לביזור עומסי עבודה ולאיזון המשאבים של הארגון על פני עננים פרטיים וציבוריים. |
| ענן פרטי | תצורה בה הארגון מחזיק ושומר על משאבי מחשוב הענן שלו. משאבים אלה מאוחסנים בחוות השרתים של הארגון עצמו. |
| ענן ציבורי | תצורה בה המשאבים מצויים בבעלותם ומופעלים על ידי ספקי שירותים של צד שלישי. ספק הענן הוא זה שמחזיק ומנהל את כל החומרה, התוכנה ותשתיות אחרות עבור לקוחותיו. משאבים אלו משותפים בין הלקוחות של ספק הענן וחשבונותיהם. |
| קוד כתשתית (IAC) | Infrastructure as code – ניהול תשתיות המחשוב באמצעות קוד תוכנה, ולא באמצעות ניהול ידני כמקובל בתשתיות On Premises, באופן המאפשר ניהול ובקרה, שכפול ושימוש חוזר ללא טעויות אנוש. |
| קונטיינר וירטואלי (Container) | 'קונטיינר' הינו רכיב המאגד בתוכו קבצי אפליקציה ומאפשר וירטואליזציה קלת משקל ברמת מערכת ההפעלה. קונטיינר הפועל על מערכת ההפעלה המארחת, הוא יחידת תוכנה סטנדרטית האורזת קוד ואת כל התלות שלו, כך שיישומים יכולים לפעול במהירות ובאמינות. |
| תפיסה אג'ילית | שיטת עבודה איטרטיבית אשר מאפשרת לנהל פרויקטי תוכנה ותהליכי פיתוח כך שהלקוח מקבל מענה לצרכיו בצורה יעילה ומהירה יותר. לעומת שיטות עבודה קודמות אשר כללו בגרסה אחת הרבה מאוד שינויים, צוותים אג'יליים מספקים גרסאות קטנות יותר, אך יותר ממוקדות לקוח. |

# נספח ב | עקרונות לסיווג מידע במעבר לענן

## רקע ומטרה:

כחלק מתהליך המעבר לענן, על משרדי הממשלה לבצע הערכת תאימות יישום לענן הציבורי (cloud suitability), ולבחון, בין היתר, את סיווג המידע במערכת, קריטיות המערכת, הרגולציה והסיכונים החלים עליה. סיווג המידע הוא שלב יסוד בתהליך זה. מטרת המסמך שלהלן היא להתוות עקרונות מסגרת לשלב סיווג המידע בלבד, וליצור שיטה קבועה ומוסכמת שתקבע את תהליך סיווג המידע בארגון בעת המעבר לענן, ובכלל זה הצגת רמת הסיווג באופן קצר וחד ערכי. עקרונות אלו יהוו בהמשך בסיס לקביעת מדיניות והגדרות הנוגעות למעבר יישומים לענן ציבורי במסגרת פרויקט נימבוס.

עקרונות סיווג המידע שלהלן ישמשו כבסיס להגדרת מדיניות וקבלת החלטות במסגרת התהליך הרחב של מעבר לענן, הן ברמת המדיניות הממשלתית הרוחבית והן ברמת הארגון והיישום הפרטני. בהיבטי המדיניות, סיווג המידע ישמש כבסיס להגדרת התנאים, התהליכים וההנחיות לאישור מעבר יישום לענן, לרבות השאלה באילו מקרים ניתן להשתמש בשירותי ענן המצויים מחוץ לריבונות ישראלית. ברמה הפרטנית, סיווג המידע ישמש את הארגון, בין היתר, לקביעת תאימות יישומים לענן במסגרת שלבי התכנון, להגדרת אמצעי ההגנה הנדרשים ולקביעת מנגנון ניהול ההרשאות בהתאם לרמת הסיווג שנקבעה.

בהמשך למסמך זה תפורסמנה הנחיות מפורטות לקביעת סיווג יישום לצורך מעבר לענן, לרבות שיקולי קריטיות והערכת סיכונים.

## 1. עקרונות לסיווג מידע:

מסמך זה מגדיר את רמות סיווג המידע למידע בסיווג בטחוני בלמ"ס בלבד, ומתבסס, בין היתר, על הצעת חוק לתיקון 14 לחוק הגנת הפרטיות, תשמ"א-1981. במטרה להקל על תהליכי סיווג מידע ומערכות עתידיים, על המשרד לנהל טבלה המכילה את סיווגי המידע השונים שברשותו. טבלה זו תאפשר סיווג מהיר יותר של מערכות נוספות המשתמשות במידע, וכן עדכון הסיווג בהתאם לשינויי המדיניות מעת לעת.

1.1 כל מידע ביישום, קיים או עתידי, המיועד לעבור לענן, יסווג לפי רמות הסיווג שתקבענה במסמך זה. הסיווג יחול על כל מידע ביישום, ללא קשר למקור או בעלות.

1.2 כחלק מסיווג המידע, יש לפרט את ישויות המידע והתחומים העסקיים הרלוונטיים למידע ביישום, על פי הנחיות מיפוי נכסי המידע שיפורסמו על ידי מערך הדיגיטל הלאומי כחלק מתהליך המיגרציה.

1.3 על המשרד לנהל טבלה של המידע שסווג והנמקה לסיווג (ישויות מידע, רמת רגישות) ולעדכנה עם כל סיווג יישום, בהתאם לנהלים הממשלתיים שיפורסמו ע"י ה-CCoE. המאגר המעודכן יתעד את תהליך אישור היישומים לענן ויאפשר עקביות בסיווג נתונים.איגום משאבים באמצעות שימוש בשירותים משותפים בענן.

1.4 אחת לתקופה, או בעת שינויים רגולטוריים, תסקר מדיניות סיווג המידע הממשלתית ובעת הצורך תעודכן במסמכיה ובמערכות המידע. על המשרד לוודא עדכניות סיווג המידע בהתאם לעדכונים אלו.

1.5 סיווג שנקבע ע"י גורמי חוץ לגבי מידע המגיע מאותם גורמים והמצוי בידי הארגון – בקבלת מידע מגורם חוץ, יש לערוך בחינה של תוכן המידע ולסווגו בהתאם לשיקולים המפורטים מטה, בהתאם לעיקרון בסעיף 2.2.

## 2. רמות סיווג מידע:

סיווג המידע מתחלק ל-4 רמות, בהתבסס על אופי המידע ותוכנו. רמות הסיווג נעות מהנמוך ביותר לגבוה לפי מידת רגישות וחומרה, הן לגבי אופי המידע והן לגבי חומרת הנזק הפוטנציאלי.

רמות הסיווג והגדרותיהן יבחנו מעת לעת ויעודכנו על ידי ה CCoE.

### 2.1 סיווג אופי המידע[9]

| רמה | אופי המידע | |
|---|---|---|
| 1 | **מידע פומבי** | מידע שפורסם באופן חוקי לציבור או מידע המותר לפרסום לכלל הציבור על פי דין |
| 2 | **מידע פנימי** | ככלל, מידע הנוגע לענייניה הפנימיים של הממשלה, המיועד לשימוש פנימי בארגון או בין מספר ארגונים, שאין לפרסמו לכלל הציבור **ואינו** מכיל מידע פרטי או מידע פרטי בעל רגישות מיוחדת, יסווג כמידע פנימי. |
| 3 | **מידע פנימי מוגבל** | מידע המיועד לשימוש פנימי בארגון וחלות עליו הגבלות על פי חוק (לדוגמה, סודיות מסחרית), תקנות (לדוגמה, תקנות חובת המכרזים) רגולציה ייעודית או הסכם<br>**או**<br>מידע פרטי שאינו מידע בעל רגישות מיוחדת. |
| 4 | **מידע פנימי חסוי** | מידע פרטי בעל רגישות מיוחדת. |

[9] המתאם בין אופי המידע לרמת הרגישות בטבלת סיווג המידע מבוסס על טבלאות דומות המקובלות בעולם בהתייחס לסיווג נתונים. חלק מסוגי המידע ( למשל, מידע פרטי או מידע על עניינים פנימיים של הרשות) בעלי מנעד רגישות רחב, ובמקרים מסוימים הדבר עשוי להשפיע על המתאם. במקרים כאלו, על המשרד הממשלתי להפעיל שיקול דעת, ולקבוע את רמת סיווג המידע בהתאם לנסיבות.

## 2.2 שיקולים לבחינת סיווג מידע:

סיווג המידע לצורך בחינת המעבר לענן יתבסס על שיקולים הנוגעים לאופי המידע ותוכנו, ובכלל זה פומביות המידע ושיקולי פרטיות. לצורך התוויית שיקול הדעת בעת בחינת סיווג המידע המתאים ליישום, ניתן להיעזר בפרמטרים המפורטים להלן:

### 3.1 פומביות המידע

3.1.1 האם ביישום קיים מידע בסיווג בטחוני גבוה מבלמ"ס?

3.1.2 האם למידע קיים חיסיון על פי דין (חוק, תקנות או דרישות רגולציה)?

3.1.3 האם המידע מפורסם לציבור כיום?

3.1.4 האם קיימת מניעה משפטית לפרסום המידע לציבור?

### 3.2 פרטיות המידע

3.2.1 האם הנתונים מכילים מידע פרטי כהגדרתו במסמך זה?

3.2.2 האם הנתונים מכילים מידע פרטי בעל רגישות מיוחדת כהגדרתו במסמך זה?

3.2.3 האם המידע מכיל מזהים ישירים?

3.2.4 האם המידע מכיל מזהים עקיפים?

### 3.3 פוטנציאל הנזק

על הארגון להביא בחשבון גם את פוטנציאל הנזק שיכול להיגרם כתוצאה מאובדן, דליפה, או שיבוש המידע במערכת. לדוגמה:

- חשיפת מידע אסטרטגי לישויות מדיניות זרות (מדינות, רשויות או ארגונים בינ"ל)
- ההשפעה על המשק, הטיה או מתן יתרון תחרותי במשק
- הפרה או אי עמידה ברגולציה קיימת
- פוטנציאל לפגיעה בגוף או בנפש
- פוטנציאל לפגיעה ביחסי החוץ של המדינה

### 3.4 אופי השימוש במידע בענן

ככלל, סיווג המידע ביישום מבוסס על אופי המידע ותוכנו, כמתואר בסעיף 4 לעיל. עם זאת, קיימים תרחישי שימוש בענן או אמצעים הממתנים את הסיכון, אשר עשויים להשפיע על רמת הסיווג, להחמירה או להקל. לדוגמה:

3.4.1 האם השימוש בנתונים בסביבת פיתוח/בדיקות בלבד?[10]

---

[10] ככלל, בסביבת פיתוח ובסביבת בדיקות לא ייעשה שימוש בנתוני אמת מלאים.

3.4.2 האם הנתונים עברו תהליך התממה?

3.4.3 האם הנתונים בענן הם נתוני דמה (מידע סינתטי)?

3.4.4 האם הנתונים במעבר בלבד או מאוחסנים בענן?

3.4.5 עד כמה המידע במערכת מקיף? מידע מקיף יכול להכיל מידע ממקורות שונים על אותה הישות, או מידע רב היכול לגרום לנזק במקרה של חשיפת המידע או שינוי שלו.

3.4.6 האם עיבוד או ניתוח המידע עשוי לייצר תובנות חדשות על נשואי המידע אשר ישנו את סיווגו?

בעת קביעת סיווג המידע למערכת, כשלב משלים, על משרד לבחון האם וכיצד משפיע תרחיש השימוש על סיווג המידע.