ניהול סיכונים, ציות ובקרה בענן	
פרק ראשי : מסמכי מדיניות CCoE	
פרק משני : GRC	

1. תוכן העניינים

2. מטרת המסמך

מסמך זה יכלול את הקווים המנחים והעקרונות בנושא ניהול הסיכונים, המשילות והציות (GRC) בעבודה בענן. עקרונות המסמך מספקים מסגרת כללית לשותפים בענן הממשלתי, והשותפים בענן יוכלו להתאים אותו בהתאם לנסיבותיהם הייחודיות.

3. קהל היעד

מסמך זה מיועד עבור בעלי תפקידים הרלוונטיים לתהליכי ניהול סיכונים, ציות ובקרה בענן (כגון: מנמ"רים, מנב"טים, יועמ"שים, מנהלי אגף טד"ם וכו'), האגפים המקצועיים במשרדי הממשלה וגורמי המטה האחראים על הפרויקט במשרדי הממשלה ויחידות הסמך.

פרק במסמך	**קהל יעד**
מדיניות הממשלה בענן בתחום משילות (Governance)	מנמ"רים, מנב"טים, גורמי מטה
מדיניות הממשלה בענן בתחום ניהול סיכונים (Risk Management)	מנמ"רים, מנב"טים, גורמי מטה, מנהלי סיכונים
מדיניות הממשלה בענן בתחום ציות (Compliance)	מנמ"רים, מנב"טים
תקנות ורגולציה בינלאומית לענן (International Regulation Policies)	יועמ"שים, מנמ"רים

למסמך זה מצורף בנספח א' אוגדן מסמכי מדיניות הגנת הסייבר הממשלתית לענן, עבור מנהלי רשת, תקשורת, אבטחת מידע וסייבר באגפי טד"ם במשרדי הממשלה השונים ובמערך הדיגיטל.

4. מונחים והגדרות

4.1. משילות בענן

התוויית מדיניות והנחייה של משרדי הממשלה ויחידות הסמך (להלן "המשרד"), בנוגע לביצוע הגירה ושימוש מוגן בסייבר בענן ציבורי.

ברמה המעשית, זהו מכלול הנחיות בנושאי מדיניות, תהליכים, מנגנונים, בעלי תפקידים, טכנולוגיות תומכות, מדדים ואמצעי בקרה אשר מאפשרים הכוונה וניהול מבוקר ומפוקח של תהליך המיגרציה לענן, הוספה והסרה של מערכות ורכיבים בהתאם לצורך, כמו גם נושאי הגנת הסייבר, תיאום יעיל של פעילויות הגנת סייבר בענן, הבטחת רמת הגנה נאותה בכל משרדי ומערכות הממשלה בענן והשגת מטרות הממשלה במעבר לענן.

4.2. מושגים הקשורים בציות בענן

א. תקינה (Standard): תקן, מפרט או שיטה מקובלים, ולעיתים גם מחייבים, ליישום בתחום מסוים.

ב. ציות (Compliance): עמידה בדרישות התקינה הקבועות.

ג. הבטחת ציות (Assurance): מנגנונים לווידוא ולהוכחת הציות.

5. מדיניות הממשלה בענן בתחום משילות (GOVERNANCE)

רכיבי מודל משילות בענן נימבוס הממשלתי:

5.1. ניהול מדיניות הממשלה בענן

<u>גורם אחראי</u> – מערך הדיגיטל בהתאם להחלטת הממשלה 2443

<u>גורם מונחה</u> – המשרד

<u>התהליכים</u>:

א. הגדרת המדיניות וניהולה - ע"י הגורם האחראי.

ב. יישום וקיום מלא של המדיניות באופן מתמשך (כולל מערכות הענן) – ע"י המשרד.

ג. כחלק מהתשתית למימוש מדיניות הממשלה בתחום המשילות, מערך הדיגיטל יספק שירות ממשלתי משותף של ניהול וניטור של תשתיות ענן מרכזיות, אשר במסגרתו יופעלו לטובת משרדי הממשלה ויחידות הסמך אזור נחיתה (Landing Zone) ממשלתי משותף, הפועל 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 <u>בהוראת התכ"ם מס' 16.2.2. פרויקט נימבוס</u> - 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 <u>להחלטת הממשלה מס' 231</u> המפרטים את התשתיות הנדרשות להקמה מרכזית בענן הציבורי ואת ייעודן כשירות רוחבי.

יובהר, המשרד נושא באחריות מלאה לקיום המדיניות בענן בכלל ובהגנת סייבר בפרט.

ד. המשרד רשאי להסתמך על בקרות קיימות, כלומר בקרות שמספקות ספקיות הענן או הגורם הממשלתי המפעיל שירות משותף, אך באחריותו לוודא מראש ולפקח באופן שוטף כי בקרות אלו אכן מתקיימות.

5.2. **מוכנות משרדית – הון אנושי**

<u>גורם אחראי</u> – המשרד

<u>התהליכים</u>:

א. בהתאם למסמך <u>מודל ההפעלה בענן – בהיבט התהליכים וההון האנושי</u> - המשרד יעסיק או יפעיל כוח אדם מיומן ובעל ידע וניסיון בתחומי GRC בענן, להבטחת עמידה בדרישות אבטחת מידע ותקינה, בהתאם לשיטות יישום מובילות בענן. לרבות ארכיטקט אבטחת מידע בענן ומהנדס אבטחת מידע בענן.

ב. מודל ההעסקה של כוח אדם זה נתון לשיקול הדעת של המשרד[1].

ג. המשרד יפעל לשמירה על כשירות מקצועית ועדכון הידע הקיים, ויוודא כי מוקצים לכך משאבים.

הארגונים יערכו בהתאם למדיניות תהליכי פיתוח ואבטחה לענן (SecDevOps, כמופיע בהמשך המסמך) – לצורך פיתוח במתודולוגיות Containers, Cloud Native או Infrastructure as Code (IaC) ועוד. ההכנה תכלול ידע, כ"א מיומן, כלים ותהליכים לניהול הסיכונים סביב סביבת הפיתוח וההפעלה של הקוד והרכיבים בענן.

[1] כמו כן, ניתן למצוא בפורטל ההדרכות של מערך הדיגיטל לנימבוס את תיאורי התפקיד, הכישורים הניסיון וההסמכות הרלוונטיות ותיאור משימות.

5.3. **מנגנון בחינת התאמת מערכות ואישור עקרוני למיגרציה של מערכות לענן בישראל**

האחריות על מנגנון זה מתפצלת בין שני גורמים, כמפורט להלן:

1) גורם אחראי – המשרד

התהליכים:

א. על המשרד לקיים ניתוח והערכת הסיכון ובחינת התאמת המערכת לענן, ע"י ביצוע הערכת סיכונים למידע ולמערכת ושימוש בכלים ממשלתיים לבחינת הסיכון (כגון מחשבון סיכון ותהליך סיווג דאטה ומערכות) אשר יונגשו לו כאמצעי או כשירות מרכזי.
הנחיות לעניין זה מפורטות בפרק 6 המופיע בהמשך המסמך.

ב. מיגרציה של מערכת לענן[2] תאושר על ידי ועדת היגוי ליישום אסטרטגיית הענן בהתאם להחלטת ממשלה 231 במסגרת העברת מערכת לענן, באחריות המשרד לזהות הבקרות הנדרשות בסביבת הענן הממשלתי, ולוודא שנשלחים לוגים תשתיתיים ואפליקטיביים ל-SOC הממשלתי, בדגש על לוגים של פעולות ניהול ותקשורת לדוגמא, המבוצעים בסביבת הענן. במקרים בהם הערכת הסיכון גבוהה ו/או המשרד מבקש לאשר מקרה חריג או חריגה מהמדיניות, ידרש אישור נוסף של ועדה ברמה ממשלתית.
דוגמאות למקרים אלו: בקשה לבצע הליך מיגרציה של מערכת על אף סיווגה כלא מתאימה לענן, היעדר תשתית או שירות ענן בישראל התומך בדרישות המערכת.

ג. ככלל, הגירת מערכות לענן מחויבות לעבור דרך ועדת ענן, כמפורט להלן, או בהתאם להנחיות אחרות שיפורסמו.

2) גורם אחראי – הממשלה באמצעות מערך הדיגיטל

התהליכים:

א. ועדת ענן ממשלתית – הועדה הממונה לאישור מעבר מערכות ממשלתיות לענן ציבורי בהתאם להנחיית יה"ב 5.5, בראשות יה"ב ונציגי מערך הסייבר הלאומי, ה-CTO הממשלתי, הרשות להגנת הפרטיות ומנהל הרכש הממשלתי.

ב. ועדה זו, תסקור תקופתית ובאופן שוטף ותבקר ככל שיידרש, את אופן ופרטי תיעוד הבחינות, הערכות הסיכון וההחלטות של המשרדים.

ג. בנוסף, ייבנה מנגנון ממשלתי לצורך פיקוח על מערכות SaaS, ובדגש על מערכות SaaS בשימוש נרחב ובמכרז מרכזי.

5.4. **מנגנון אישור עבור הליך מיגרציה של מערכת בפועל ומעבר לסביבת ייצור בענן בישראל**

גורם אחראי – המשרד

התהליכים:

א. בטרם מעבר המערכת לסביבת ייצור, על המשרד לבדוק את רמת ההגנה העדכנית הנדרשת בסביבת הענן בישראל וכפי שיושמו במערכת, אל מול דרישות מסגרת הבקרות האחודה שתוגדר בוועדת הענן הממשלתית. על בדיקה זו להתבצע באמצעות בקרה ממוכנת ואוטומטית לבחינה וניטור הסביבה באופן

[2] ראה מסמכי מתודולוגיית מסע לענן ממשלתית.

מקיף, רציף ומעמיק, לצורך הערכת רמת העמידה בתקנים ובדרישות, קבלת תמונת מצב, זיהוי חריגים, וזיהוי דרכי הטיפול. בקרה זו תבוצע באמצעות כלי שיסופק בעתיד על ידי מערך הדיגיטל באופן מרכזי.

ב. כמו כן, על המשרד לוודא את מוכנותו למעבר לסביבת הייצור, לרבות:

1. חיבור לשירותי ניהול זהויות, הזדהות והרשאות גישה.
2. איסוף לוגים נדרשים, העברתם לתשתית ומרכז ניטור מרכזיים.
3. הגדרת הסביבה והמערכת באופן המאפשר תגובה לאירועים.
4. זמינות כ״א מיומן המתאים לתפעול הגנת סייבר על המערכת בענן.
5. בהתאם להנחיות יה״ב, יש לבצע מבדקים טכניים שונים טרם עלייה לאוויר, ככל שרלוונטי לתצורת/מודל צריכת הענן. המבדקים הטכנולוגיים יהיו, בין היתר, סקר לאבטחת מידע בתחומי התשתית, ארכיטקטורה, ניטור, ציות, מבדקי חוסן (חדירות) ועוד. מבדקים טכנולוגיים אלו יתוקפו אחת ל-18 חודשים.
6. ככל שזוהו ממצאים קריטיים, חמורים או גבוהים, באחריות המשרד:
   - לתקן את הממצאים בתוך פרק זמן קצוב (SLA) בהתאם לרמת הסיכון.
   - לוודא את התיקון בעזרת סקירה חוזרת ממוכנת באותו אמצעי ככל האפשר.
   - לאור הממצאים וסטטוס תיקונם, לקבל את אישור הועדה הרלוונטית (פנים-משרדית, או ברמה הממשלתית, כמפורט לעיל) למעבר לייצור.
7. אם זוהו ממצאים ברמת חומרה בינונית או נמוכה, באחריות המשרד לתקנם בפרקי הזמן הבאים:
   - ממצאים ברמת חומרה בינונית - תוך חודש לאחר המעבר לסביבת ייצור
   - ממצאים ברמת חומרה נמוכה - תוך שלושה חודשים לאחר המעבר לסביבת ייצור.

ג. המשרד נדרש לבצע בקרה ממוכנת ורציפה לניטור רמת העמידה בתקנים, שיקוף תמונת המצב וזיהוי וטיפול בחריגים. הנחיות מפורטת לבקרה מופיעות בפרק 7.

5.5. **מנגנון בחינת התאמת מערכות ואישור עקרוני למערכות בענן בחו״ל, למשרדים אשר קיבלו אישור חריג ממערך הדיגיטל הלאומי.**

גורם אחראי – המשרד

התהליך:

ככלל, המערכות יהגרו לענן היושב באזור הישראלי. חריגים יאושרו כפי שכתוב בהתאם להנחיית יה״ב 5.5, ובמסגרת ועדת הענן. לטובת קבלת אישור חריג לשימוש במערכות בענן בחו״ל ממערך הדיגיטל הלאומי, על המשרדים לקיים תהליכי ניהול סיכונים בבחינת הסיכון בשימוש בסביבת ענן או במוצרי SaaS מחוץ לגבולות מדינת ישראל, ובכלים כגון מחשבון לחישוב הסיכון (כולל קבלת אישור ועדת ענן המטפלת בחריגים ובמערכות בסיכון גבוה או במורכבות גבוהה).

5.6. **קיום בקרה רציפה לאחר מעבר המערכת לייצור**

גורם אחראי – המשרד

התהליך:

כל משרד נדרש לקיים בקרה מתמשכת ורציפה על רמת העמידה בדרישות הגנת הסייבר הרלוונטיות של כל מערכותיו בענן לאורך כל מחזור חייהן.

5.7. אימוץ סטנדרט אחיד והבטחת העמידה בו (Compliance and Assurance)

גורם אחראי – המשרד

התהליך:

כחלק מהמעבר לענן, וכדי לאפשר את הבטחת איכות המידע, מצורפת רשימת תקנים רלוונטיים:

- תקן ISO27017 (אבטחת מידע בענן)
- תקן ISO27018 (הגנת פרטיות בענן)
- תורת ההגנה בסייבר 2.0 (מערך הסייבר הלאומי)
- הנחיית יה"ב 5.3 ניהול סיכוני סייבר
- מטריצת בקרות ענן על ידי שותפות הגנת הענן (Cloud Controls Matrix, by CSA)

להרחבה בנושא ניהול הסיכונים יש לפנות לפרק 6 במסמך זה.

5.8. מסגרת בקרות אחודה

גורם אחראי – יה"ב

התהליך:

יה"ב תגדיר ותאמץ מסגרת בקרות אחודה עבור השימוש בענן: יכולות הגנה נדרשות, בקרות הגנה והגדרה סטנדרטית רוחבית ואחודה לכל משרדי הממשלה של "מדיניות ענן טכנולוגית" ו"מעקות בטיחות" (Policies and Guardrails). מסגרת זו תכלול את הבקרות הנדרשות על פי התקנים החיצוניים, ובמידת הצורך, יתווספו אליהן נדבכים נוספים.

5.9. ניהול רמת ההגנה בענן (Cloud Security Posture Management)

גורם אחראי – המשרד

התהליך:

המשרד נדרש לקיים בקרה מתמשכת ורציפה על רמת העמידה של כל המערכות שלו בענן לאורך כל מחזור חייהן בדרישות הגנת הסייבר הרלוונטיות (כלי ההגנה יפורסמו בהתאם לכלים זמינים במסגרת רובד 5. ראה קישור).

תמונת מצב של רמת ההגנה ברמת המשרד היחיד תונגש לוועדת הענן המשרדית ובאופן רוחבי חוצה משרדים ההנגשה תתבצע לצוות הניטור והבקרה הממשלתי.

5.10. רציפות תפקודית והמשכיות עסקית

גורם אחראי – המשרד

התהליך:

המשרד נדרש לתת מענה הולם לנושא רציפות תפקודית והמשכיות עסקית במעבר לענן כחלק מהערכת התאמת המערכת לענן ועיצוב הבקרות לקראת הליך המיגרציה:

א. ברמת המערכת- נדרש מענה לתחומי גיבויים ושחזורים; רמות יתירות, זמינות ושרידות; ומנגנוני התאמת קיבולת (scale up / down ידני או auto scaling עפ"י צורך).

ב. ברמת עבודה מול ספק התשתית/פלטפורמה/תוכנה כשירות- יש לוודא כי הספק מקיים את המנגנונים אליהם הוא מחוייב[3].

ג. ברמת צריכת הענן- יש לבחון וליישם ככל הנדרש את הגדרות התצורה מול ספק הענן ואת המנגנונים המשלימים בצד המשרד.

בכדי להפחית סיכון Vendor Lock-In ולאפשר Exit Strategy מול ספק מסוים, יש לבחון ולבצע, ככל הנדרש, מנגנונים לגיבוי חיצוני לספק הענן (בענן אחר/ בעזרת מוצר או שירות ייעודיים/ בסביבת מחשוב משרדית או ממשלתית אחרת). דרישות אלה יענו בעזרת ניהול וניטור שוטף לאחר הליך המיגרציה והמעבר לסביבת הייצור, ובעזרת בקרה ותרגול תקופתיים.

5.11 שירותים משותפים

גורם אחראי –מערך הדיגיטל

התהליך:

הממשלה תקים ותנגיש שירותים משותפים למשרדים עבור המערכות בענן, לצורך משילות הגנה בענן, הפחתת סיכונים, חיזוק ההגנה בפועל, יעילות תפעולית, הקלה על המשרדים בהליך המיגרציה ובשימוש בענן, הקטנת תקרות וחיסכון בזמן, מאמצים ועלות.

השירותים המשותפים יכללו: אזור נחיתה ממשלתי, מימוש מדיניות ממשלתית באמצעות קוד (Policy as Code),פריסת תשתית באמצעות קוד ואוטומציה (Infra as Code), מוצרי אבטחת מידע, שירותי אבטחה תפעוליים וחנות (Marketplace) לאפליקציות שאושרו לצריכת המשרדים.

ככלל, המשרדים נדרשים להשתמש בשירותים הממשלתיים המרכזיים העומדים לרשותם כחלק מפרויקט נימבוס. משרד אשר יעדיף שלא להשתמש באזור הנחיתה הממשלתי, יידרש לקבל אישור מיוחד לכך ע"י מנהל הרכש ומערך הדיגיטל. לא ינתנו אישורים חריגים לאי שימוש ב-SOC ממשלתי, כולל מערכות התוכנה המשרתות אותו (כגון אגירת לוגים, SIEM), התחברות לכלים מרכזיים המאפשרים Security Posture Management (ניהול רמת ההגנה) והתחברות למערכת IAM (ניהול זהויות והרשאות גישה). אישור מיוחד לאי שימוש באזור הנחיתה המשותף בהיבטי סייבר ידרוש הוכחת מוכנות ובשלות, עמידה בכל דרישות מדיניות הגנת הסייבר, הגדרת תצורה וגישה המאפשרת ניטור, סקירה וביקורת של סביבות הענן של המשרד בהיבט של הגנת סייבר וניטור סייבר.

5.12 התאמת מודל האחריות המשותפת[4]

גורם אחראי – מערך הדיגיטל ומשרדי הממשלה

התהליך:

מודל האחריות המשותפת מורכב משני חלקים:

א. מודל אחריות משותפת בין המשרד לבין ספק שירותי הענן

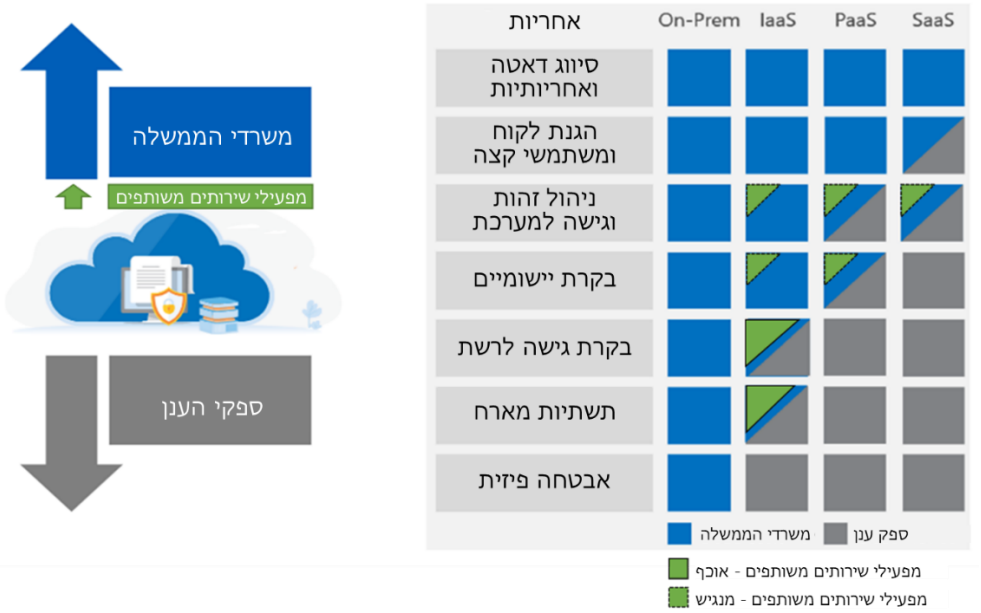
[3] ראה הוראת תכ"מ 16.2.2 – פרויקט נימבוס

[4] ראה גם מסמך מודל הפעלה בפן הטכנולוגי

ב. במקרים בהם המשרד משתמש בשירותים המשותפים- התחומים שהיו באחריות המשרד מתחלקים בינו לבין הגוף הממשלתי המפעיל את השירותים המשותפים:

1. ברבדים התשתיתיים – Host, Network – אזור הנחיתה המשותף מגדיר ואוכף בקרות.
2. ברבדי המערכת – application, identity and access – אזור הנחיתה המשותף כולל ומנגיש בקרות ומנגנונים (לדוגמא: WAF, IAM, Authentication) והמשרד ואחראי המערכת אחראיים להשתמש בהם.

תחומי האחריות המשתנים מוצגים באיור הבא:



5.13. **שפת "אבטחת מידע" אחודה**

<u>גורם אחראי</u> – מערך הדיגיטל

<u>התהליך</u>:

על מנת לסייע למשילות, תשאף הממשלה לאמץ שפת "אבטחת מידע" אחודה, בהעדפה לאימוץ סטנדרטים בינלאומים.

שפה אחידה מאפשרת לקבל תמונת מלאה, ברורה ועקבית של רמת ההגנה (posture), לבחון את אפקטיביות המדיניות והבקרות ולייעל את שיתוף הידע והמידע בין גופי הממשלה ואת פעילות גופי אבטחת המידע המרכזיים (לדוגמה: מתן מענה רוחבי מקדים, בעקבות גילוי של איום במשרד אחד). באחריות יה"ב להגדיר את הסטנדרטים ("השפה") ולפרסם הנחיות פרטניות בנושא.

.

"שפות" כוללות לדוגמה: MITRE ATT&CK (צעדי וטכניקות תקיפה) , OSCAL (בקרות הגנה)

5.14. **מעקב ובקרה**

<u>גורם אחראי</u> – מערך הדיגיטל

התהליך:

מערך הדיגיטל יפעיל מכלול מנגנונים ויכולות למעקב, בקרה, ואכיפה ברמת הממשלה, הכוללים: מערכת תיעוד, בקרת צרכנים, בקרת ספקים ברמה ממשלתית ברמת המשרד, ניטור רציף, איתור חריגים, מעקב יישום מול מדדים ותהליך שיפור מתמשך.

5.15. **שיפור בשלות מנגנוני המשילות - כתהליך שיפור הדרגתי**

גורם אחראי - מערך הדיגיטל

התהליך:

מערך הדיגיטל יערוך בחינות תקופתיות של מנגנוני המשילות לכלל הגורמים המעורבים בתהליך, לצורך שיפור מתמשך. הבחינות יערכו לאורך תקופה של 3 שנים לפחות, כאשר בשנה הראשונה יתקיימו בתדירות רבעונית, והחל מהשנה השנייה בתדירות חציונית.

לסיכום חלק זה של המסמך: חלוקת תחומי האחריות והתפעול בין השותפים בנימבוס מפורטת בטבלה בנספח 1 למסמך זה.

6. מדיניות הממשלה בענן בתחום ניהול סיכונים (Risk Management)

6.1. מסגרת ניהול סיכונים - מבוא

המורכבות התהליכית והטכנולוגית בענן מחייבת תפיסת ניהול סיכונים מותאמת. מורכבות זו נובעת ממודלי השירות השונים בענן, משמעות האחריות המשותפת בכל אחד בהם, ותצורות מגוונות של צריכת שירותי ענן שונים. כל אלו הופכים את הגבולות, הממשקים ותחומי האחריות בין השותפים בפרויקט למורכבים יותר. הואיל ומנגנוני ניהול סיכונים מסורתיים וכלליים פחות יעילים בענן, יש לאמץ מתודולוגיה מותאמת, כמפורט להלן.

המסגרת הממשלתית לניהול הסיכונים בענן מבוססת על שילוב מספר מסגרות עיקריות:

א. מסגרות כלליות
   1. תורת ההגנה בסייבר 2.0
   2. הנחיית יה"ב 5.3 ניהול סיכוני סייבר

ב. מסגרות ייעודיות לתחום הענן
   1. תקן ISO27017
   2. תקן ISO27018 (הגנת פרטיות בענן)
   3. CCM

ג. מסגרות מותאמת לממשלת ישראל ולמעבר בענן במסגרת פרויקט נימבוס
   1. מסגרת ניהול סיכונים בשלוש רמות: ממשלתית, משרדית, ומערכת בודדת
   2. ניהול מדיניות הממשלה בענן כחלק מהליך המיגרציה לענן בכלל, ובבחינת התאמת מערכות ספציפיות לענן בפרט
   3. ניהול סיכוני הסייבר כתהליך רציף והמשכי לאורך מחזור החיים של המערכות

6.2. ניהול הסיכונים בענן ברמה הממשלתית

אסטרטגיית הממשלה עבור הליך המיגרציה לענן ציבורי והשימוש בו, כוללת מספר רכיבים, אשר נוסף ליתרונות רבים אחרים (כלכליים, תפעוליים, טכניים-מקצועיים ועוד) מגדירים את תפיסת ניהול סיכוני הענן הממשלתית ואת ספי הסיכון, ומספקים בקרות מרכזיות להפחתה ולניהול סיכונים אלו.

המשרד אחראי להעריך את רמת הסיכון המקובלת עליו (Risk Appetite), התלויה בסיבולת שלו לסיכון השיורי של השימוש בענן ובהתאמה למסמכי המדיניות ומחשבון סיווג הדאטה שהונגש על ידי מערך הדיגיטל.

ניהול רכיבים ובקרות ברמה ממשלתית מרכזית מאפשר הפחתת סיכונים באופן אפקטיבי, יעיל ואחיד, סיוע למשרדים בהליך מיגרציה מוצלח ובטוח, תוך הקטנת תקורה, ואלו כוללים:

א. הגדרה ברורה של אזורי ענן (regions) ספציפיים מחוץ לישראל (בהתאם לאישור החרגה מוועדת ענן) וקבועים בישראל, ושל סוגי המערכות והמידע אשר יכולים להתארח בהם.

ב. הקמת מרכז מצוינות לענן (CCoE) אשר מגדיר אסטרטגיה, מדיניות, בקרות והנחיות עבור הליך המיגרציה ושימוש בענן לכלל הממשלה, תוך שילוב פרקטיקות מובילות עם צרכים ושיקולים אשר חלים על כל חלקי הממשלה באופן רוחבי והקמה ותפעול של אזור נחיתה הממשלתי ושירותי ניהול ענן והגנת ענן משותפים.

ג. סיכוני סייבר בפרט - הגדרה ממשלתית מחייבת של מודל תפעולי, משילות, תחומי אחריות, ספי סיכון מקובלים, הנחיות ניטור וניהול סיכוני סייבר, בקרות נדרשות ומדיניות הגנת סייבר המתייחסת לאזורי הענן הזמניים והקבועים.

ד. רכש של כלי ניטור, הערכה וניהול רמת הגנת הסייבר בענן (יירכש בעתיד ע"י מערך הדיגיטל)

ה. שירותים מרכזיים ע"י צוות רוחבי ממשלתי (כגון תשתית ניהול זהויות והרשאות (IAM) מרכזית, הרחבת מרכז הניטור הממשלתי (SOC) לכיסוי צריכת הענן הממשלתית והקמת צוות תגובה לאירועים).

ו. בחינה תקופתית וערענון המדיניות וההנחיות בהתאם להתפתחות הטכנולוגית בענן, איומים חדשים, לקחים מהתהליך וזמינות שירותים חדשים מספקי הענן בתקופת הביניים, עד שיירכשו כלים מרכזיים, ייעשה שימוש בכלי ניטור הניתנים ע"י ספקי הענן על בסיס מדיניות והנחיות מפורטות שייקבעו.

6.3. ניהול הסיכונים ברמה המשרדית

א. המשרד אחראי לניהול מדיניות הממשלה בענן ברמה המשרדית וברמת כל מערכת על פי דרישות המדיניות הממשלתית כמפורט במסמך זה.

ב. כמתואר בפרק "משילות" (פרק 5 לעיל), מתקיים מנגנון הורשה: משרד יכול להחמיר את הדרישות הכלל-ממשלתיות ברמת המשרד או המערכת הבודדת, אך לא להקל ביחס לדרישות מכרז נימבוס.

ג. המשרד אחראי על יישום וניהול הגנת המערכות ושירותי הענן עפ"י דרישות המדיניות הממשלתית.

ד. המשרד אחראי לוודא כי עומדים לרשותו הידע וכוח אדם, התהליכיים והטכנולוגיים הנדרשים לקיום דרישות המדיניות של הממשלה בענן ולהגנת סייבר.

ה. המשרד נדרש להשתמש בספקים מאושרים שנבחרו במכרזים מרכזיים

ו. ככלל, המשרדים נדרשים להשתמש בשירותים ממשלתיים מרכזיים העומדים לרשותם כחלק מפרויקט נימבוס, לרבות אזור הנחיתה הממשלתי.

6.4. ניהול הסיכונים בענן ברמת המערכת והתהליך העסקי

א. בתכנון מערכת מידע מבוססת ענן, הליך מיגרציה של מערכת קיימת לענן או אימוץ שירות ענן - משרדי הממשלה הם הבעלים של המידע הקיים במערכות, ונשארים אחראים לאבטחת המערכת והנתונים בהתאם לרגישותם יחד עם ספק הענן וספק השירות המשותף, בהתאם לחלוקת תחומי האחריות המתוארת בסעיף 7.3.

ב. תהליך זה יבוצע בהתאם למתואר במסמך "סיווג דאטה ומערכות" ובאמצעות שימוש במחשבון "סיווג דאטה ומערכות" שבאמצעותו משרדים יכולים לקבל הכוונה לרמת הסיכון של המידע והמערכת בענן.

ג. עם זאת, רמת השליטה והניהול הישיר של המשרד משתנה בהתאם למודל פריסת הענן ולמודל השירות הנבחר. במודל IaaS בקרות מועטות יותר באחריות הספק ובקרות רבות יותר באחריות המשרד, ולהיפך במודל SaaS. מודל האחריות המשותפת הכללי המותאם לנימבוס מתואר בפרק "משילות" בסעיף "התאמת מודל האחריות המשותפת".

6.5. ניהול הסיכונים בענן ברמת המערכת – רכיבי מפתח

לאור המורכבות המובנית במודל האחריות המשותפת הוגדרו מספר תחומי אחריות למשרדים, לטובת ניהול אפקטיבי של מדיניות הממשלה בענן עבור מערכת מידע:

א. קיום תהליך הערכה ותכנון הכולל ניתוח והערכת הסיכונים, בחינת התאמת המערכת לענן, בחירת מודל שירות הענן ותצורה ובחירת אסטרטגית המיגרציה לענן.

ב. זיהוי רמת ואמצעי הגנה נדרשים מותאמי-סיכון.

ג. תיחום ברור ופרטני של גבולות ואזורי אחריות בין ספק תשתית/שירות הענן, מערך הדיגיטל (כספק שכבת שירותים משותפים ואזור נחיתה) והמשרד.

ד. וידוא, כי ספק הענן מקיים את הבקרות שבאחריותו, בעזרת המסגרת החוזית, תכנון פרטני וניטור.

ה. יישום תצורות, בקרות ובקרות-מפצות מצד המשרד.

ו. פיקוח באופן רציף על קיום הבקרות.

6.6. ניהול מדיניות הממשלה בענן ברמת המערכת כחלק מהליך המיגרציה[5]

ניהול אפקטיבי של מדיניות הממשלה בענן מחייב שילוב פעילויות, בשלבים הרלוונטיים, בתזמון המתאים ותוך שיתוף פעולה בין בעלי התפקידים השונים, כמודגם בטבלה הבאה:

הליך המיגרציה	היערכות והכנה	בדיקת התאמה	תכנון	ביצוע	מוכנות לשימוש ותחילת שימוש
ניהול סיכוני סייבר	לימוד הסיכונים, תכנון, מיפוי ושילוב כבר בשלב ההיערכות לרבות רכש ויישום של בקרות אבטחת מידע נדרשות בהתאם לסיווג המידע במערכת.	סיווג מערכת ניתוח סיכון שורשי	זיהוי בקרות	יישום בקרות הערכת בקרות וסיכון שיורי	אישור השימוש

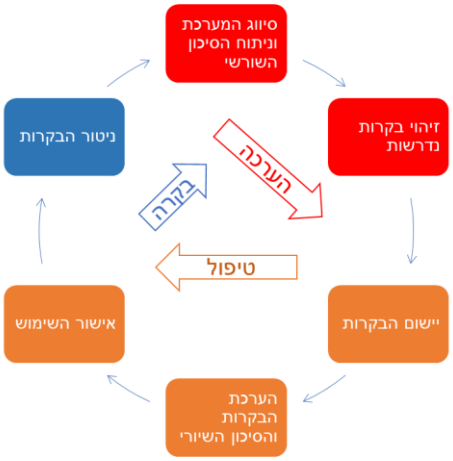
לטבלה המפרטת את פעילויות ניהול סיכוני הסייבר בשלבי המיגרציה השונים, ראה נספח 2 למסמך זה.

6.7. ניהול סיכוני סייבר בענן כתהליך רציף והמשכי

א. מבוסס על הנחיות כלליות לניהול סיכוני סייבר במערכת (תוה"ג 2.0, הנחיית יה"ב 5.3, NIST), הנחיות הקשורות ספציפית לענן (ISO-27017-8, NIST) והתאמות לפרויקט הנימבוס.

ב. לאחר הליך המיגרציה והמעבר לסביבת הייצור, ניהול סיכוני הסייבר מבוצע כתהליך המשכי לאורך מחזור חיי המערכת או התהליך העסקי, כולל ניטור רציף ותקופתי. במסגרת תהליך זה, נבחנות ומבוצעות התאמות, ככל שנדרש, בכל שלבי ורכיבי ניהול הסיכונים, כמפורט בתרשים שלהלן:

[5] ראו גם מסמך היערכות משרדית למיגרציה לענן:
https://www.gov.il/he/departments/policies/office_preparation_for_cloud_migration



ג. הפעילויות הנדרשות מהמשרד, ברמת המערכת, להתאמת מסגרת ניהול סיכונים כך שתהיה אפקטיבית עבור מערכות בענן, כוללות: סיווג, זיהוי בקרות, יישום בקרות, הערכת הבקרות, אישור שימוש וניטור. לפירוט בנושא זה, ראו נספח 3.

6.8. **התאמת ניהול סיכוני הסייבר לאופן צריכת שירותי הענן ע"י הממשלה**

ניהול אפקטיבי ורציף של הסיכונים מחייב התייחסות, בכל הרמות (ממשלה, משרד, מערכת), לתצורות צריכת הענן הרלוונטיות במסגרת פרויקט נימבוס (התאמת ניהול הסיכון לתצורה ספציפית או לעצם ריבוי התצורות)

כמו כן, יש להשתמש במחשבונים לחישוב סיכון וסיווג מידע ומערכות לצרכי הערכת הסיכון והתאמת ניהול הסיכון למצב, כהכנה לוועדת הענן הממשלתית. יש להתייחס לנושאים: ריבוי המשרדים, ריבוי עננים וספקים, שימוש בכל מודלי השירות (תשתית, פלטפורמה, תוכנה כשירות) ובמגוון מוצרי צד ג' וכן למיקום גיאוגרפי בחו"ל מול מיקום בישראל.

6.9. **סיווג מערכות, מידע ונכסי מידע לצורך הערכת הסיכון**[6]

א. ניתוח והערכת הסיכון יתקיים ברמת המערכת או התהליך העסקי.

ב. ניתוח והערכת הסיכון השורשי מסתמך על הערכת הנזק האפשרי מהתממשות הסיכון (Impact), ובסבירות להתממשותו (Likelihood).

ג. ניתוח הסיכון מבוסס על מספר היבטים או שאלות עיקריות ומדרג תשובות אפשרי.

ד. שימוש בכלים רוחביים של הממשלה בשיטה אחידה לסיווג רגישות המידע וסיכוני המידע והמערכות אשר מתוכננות לפעול בענן.

6.10. **ניהול הגנה מבוסס-סיכון**

עפ"י מסגרת ניהול סיכוני הסייבר בענן, על בקרות ההגנה להיות מבוססות סיכון:

א. על פי הערכת רמת הסיכון של המערכת באופן כללי

ב. בהתאם לסוגי הסיכונים הרלוונטיים כפי שנותחו באופן פרטני

[6] ראה מסמך סווג דאטה ומערכות (קישור יוצמד כאשר המסמך יופץ)

7. מדיניות הממשלה בענן בתחום ציות (COMPLIANCE)

7.1. מבוא ומטרות

עולם הציות מתחלק לשני היבטים עיקריים: ציות חיצוני (לחוקים, לתקנות וכו') וציות פנימי (נהלי החברה, מדיניות, כללים שהוגדרו מראש). פרק זה מציג הסברים בנוגע להגדרות מקובלות בתחום הציות, המבוססות על פרקטיקות מובילות ומוכחות מהעולם, שהיוו תשתית למדיניות הממשלה בענן בתחום הציות.

הגדרות אלה נבחרו בשל התאמתן למחשוב ענן בכלל ולמאפיינים הייחודיים של מעבר ממשלת ישראל לענן בפרט. ישנה חשיבות מיוחדת בהגדרת מושגים ברורים, פשוטים ומוכרים, כדי ליצור אחידות בין השותפים השונים בפרוייקט.

פרק זה מפרט את הדרישות ממשרדי הממשלה ויחידות הסמך, לקיים מנגנון הבטחת ציות (Assurance) ולהגדיר מנגנונים תהליכיים וטכנולוגיים לווידוא ציות ועמידה בתקינה.

7.2. הגדרות לפרק הציות

א. תקינה (Standard): תקן, מפרט או שיטה מקובלים, ולעיתים גם מחייבים, ליישום בתחום מסוים.

ב. ציות (Compliance): עמידה בדרישות התקינה הקבועות.

ג. הבטחת ציות (Assurance): מנגנונים לווידוא ולהוכחת הציות.

הגדרת מנגונים הרלוונטיים לציות נדרשת לשם השגת המטרות הבאות:

א. להבטיח ששירותי הממשלה המונגשים בענן יספקו רמת אבטחה גבוהה.

ב. לייצר אצל ציבור לקוחות ומשתמשי המערכות ביטחון ואמון במערכת מאובטחת, המקיימת ציות לתקן בינלאומי מוכח ומקובל, שעברה בדיקות איכות מקפידות, ונסקרה ע"י בודק חיצוני בלתי תלוי.

ג. ליצור אחידות אצל כלל שותפי הפרוייקט כאמצעי תומך ומשילות.

7.3. חלוקת תחומי אחריות

א. בתחום הקמת מערכות מידע מאובטחות בענן, האחריות על אבטחת המידע נחלקת בין כמה גורמים, במודל האחריות המשותפת:

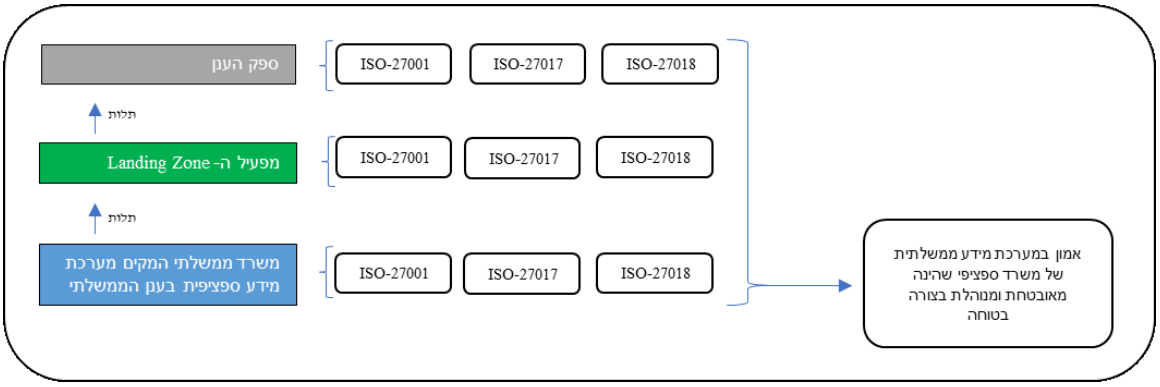
1. ספק הענן (תשתית כשירות או פלטפורמה כשירות - Google GCP, Amazon AWS) או ספק התוכנה כשירות
2. ספק השירות המשותף או אזור נחיתה ממשלתי או משרד המקים אזור נחיתה עצמאי
3. צרכן השירות (המשרד הממשלתי והשותף הרלוונטי בפרויקט)

ב. האחריות לציות נחלקת למספר רבדים, אשר על כולם להתקיים כדי שמשרד ממשלתי יוכל לקיים ציות ולהציג עדות לכך:

1. <u>אחריות ספק הענן</u> – לעמוד בתקני הבטחת מידע.
2. <u>אחריות מערך הדיגיטל על אזור הנחיתה הממשלתי</u> - לעמוד בתקני הבטחת איכות לגבי כל תשתית האירוח שהקים והמערכות המשיקות לה. אחריות זו תחול גם על כל שותף בפרויקט אשר יקים לעצמו איזור נחיתה פרטי כלל משרדי.
3. <u>אחריות משרד ממשלתי</u> – משרד ממשלתי המקים מערכת מידע בתשתית אזור הנחיתה הממשלתי בענן יוודא שהמערכת אותה הקים עומדת בדרישות של תקני הבטחת איכות בתחום

הגנת הסייבר והפרטיות. בנוסף, עליו לוודא כי התהליכים הרלוונטיים במשרד אשר קשורים להעלאת המערכת וניהולה השוטף עומדים גם הם בתקנים המצויינים במסמך זה. המשרד יוודא את האמור גם לגבי ספקי וקבלני המשנה שלו הפועלים מטעמו.

ג. משרד ממשלתי אשר רוצה להציג קיום ציות ולהציג עדות לווידוא הציות, חייב לוודא שכל הגורמים לעיל מציגים אסמכתאות לעמידה בתקנים. מודל זה ידוע כמודל "**בקרות צוברות**": בקרות נצברות מהרמות והרבדים השונים, והגורם האחראי לשכבה מסוימת יכול לרשת ולהסתמך על בקרות שנצברו מהרמות שמעליו:



7.4. **תקינה רלוונטית עבור הגנת סייבר בענן**

<u>גורם אחראי</u> – כל משתמשי הענן.

מומלץ לעמוד בדרישות תוה"ג 2.0, בתקנים הבינלאומיים ISO-27017 ו- ISO-27018.

7.5. **מנגנון תהליך ההסמכה וקבלת תעודה על עמידה בדרישות איכות**

<u>גורם אחראי</u> – המשרד

<u>התהליך</u>:

א. בהתאם להנחיות יה"ב לפחות אחת ל-18 חודשים - יעביר המשרד הממשלתי את כל מערכותיו שבענן תהליך אשרור ובחינת המצב הקיים אל מול התקנים שנבחרו כדי לוודא עמידה בדרישות התקנים.

ב. בנוסף לאמור בסעיף א' לעיל, היה ובמהלך הזמן שבין מבדק למבדק, מערכת קיימת בענן עברה שינוי מהותי או הוקמה מערכת חדשה, יוודא המשרד <u>לפני</u> עלייה לאוויר שהמצב הנתון החדש של המערכת עומד גם הוא בדרישות התקנים.

ג. המשרד יהיה רשאי להשתמש במומחים ויועצים כדי לסייע לו לעבור את המבדק הרשמי בהצלחה.

ד. המשרד יוכל להציג תעודות עמידה בתקנים, (לדוגמה: הצגה של תעודת תו תקן בדף מיוחד באתר של מערכת מידע מוחצנת מהענן) ו/או באופן גורף עבור כל המערכות שלו בענן, ע"י הצגת תו/ תעודה המעידה על עמידה בתקנים, בתנאי שהוסמך באופן רשמי כך שהציג במבדק הרשמי הוכחות לכך שכלל מערכותיו שבענן עומדות בדרישות התקנים, אלא אם כן הסמיך רק חלק מהן ובמצב זה יוכל להציג תעודות עמידה בתקנים רק למערכות אותן כיסה במבדק.

7.6. **שימוש במנגנונים אוטומטיים לווידוא אכיפת איכות רמת הגנת הסייבר**

<u>גורם אחראי</u> – המשרד

<u>התהליך</u>:

א. מאחר שתהליך ההסמכה אינו מתרחש באופן רציף אלא אחת לתקופה, קיים סיכון שבתוך חלון הזמן שבין מבדק למבדק, רמת איכות הגנות הסייבר והפרטיות תישחק, יווצרו פערים מול התקינה ותתקיימנה חשיפות באבטחת המידע. בכך תהיינה המערכות והמידע שבהן בסיכון מפני תקיפות סייבר, חשיפת מידע ו/או שיבושו.

ב. כדי לתת מענה רציף לסוגיות אלו ולהשלים את התמונה הכוללת והמערכתית של ניהול הבטחת איכות הגנת סייבר והגנת הפרטיות, נדרשים המשרדים ליישם כלים אוטומטיים להגנה ואכיפה רציפה:

- ברמה המניעתית - נדרש יישום תשתית כקוד (IaC) ומדיניות כקוד (PaC) המאפשרות קידוד מדיניות בקבצי תצורה ומיכון יישום ואכיפת בקרות.
- ברמת הניטור, גילוי וטיפול בממצאים חריגים - יופעלו מערכות המנטרות את תשתיות הענן ומוצרי אבטחת המידע ע"י מפעיל השירותים המשותפים כדי לזהות בזמן אמת חריגות מהנחיות בתקנים השונים בכל מערכת וסביבה. כחלק מתהליך הרציף של העמידה בדרישות התקן, המשרד הרלוונטי יטפל בליקוי שזיהתה המערכת האוטומטית. ראו הגדרות בפרק 5 "משילות" בסעיף "ניהול רמת הגנת הסייבר (Security Posture)".

7.7. **לוחות זמנים ליישום המדיניות**

<u>גורם אחראי</u> – המשרד

<u>התהליך</u>:

א. המשרד מחוייב לסיים את תהליך ההסמכה הרשמי, הכולל אשרור והנפקת תו תקן על ידי גורם צד ג' רשמי ומוסמך לפי התקנים שנבחרו, עבור כל המערכות בענן של המשרד תוך 6 חודשים לכל היותר מיום עליית המערכות לאוויר.

ב. המשרד ינהל, החל מתחילת הקמת המערכת ותוך שלבי ההפעלה שלה, תוכנית בקרה לווידוא עמידה בתקנים, כך שביום עליית המערכת לאוויר יוכל המשרד להציג לגוף ממשלתי פנימי אסמכתת ביניים לכך שהדרישות בתקנים נענו.

8. תקנות ורגולציה בינלאומית לענן (INTERNATIONAL REGULATION POLICIES)[7]

מעבר משרדי הממשלה לענן במסגרת פרויקט נימבוס מהווה שינוי עמוק בהיבטי הטכנולוגיה, ארגון וחוויית הלקוח. במסגרת הליך המיגרציה, כל אחד ממשרדי הממשלה נדרש לניהול סיכונים רחב-היקף ומורכב, המכיל היבטים תפעוליים, משפטיים, טכנולוגים ועוד. מדינת ישראל מצטרפת בפרויקט זה למדינות רבות ברחבי העולם, אשר החלו בתהליכים דומים בשנים האחרונות.

הרחבות נוספות ובנצ'מארק בנספח ג'.

[7] ראה פרק רגולטורי – קישור יוצמד כאשר המסמך יופץ

9. מסמכים ישימים וקשורים

9.1. מסמך אסטרטגית ענן

9.2. בהוראת התכ"ם מס' 16.2.2. פרויקט נימבוס

9.3. להחלטת הממשלה מס' 231

9.4. מודל ההפעלה בענן – בהיבט התהליכים וההון האנושי

10. נספחים

נספח 1 – חלוקת תחומי האחריות והתפעול בין השותפים מפורטת בטבלה שלהלן:

נושא	רובד תהליכי / טכנולוגי	שותפים			
		מערך הדיגיטל	**מערך הדיגיטל הלאומי ושירותים משותפים** **<u>תשתית ופלטפורמה</u>**	**משרד הצורך אזור נחיתה ושירותים משותפים** **<u>רמה אפליקטיבית בלבד</u>**	**משרד שאינו צורך אזור נחיתה ושירותים משותפים** **<u>כל הרמות: תשתית, פלטפורמה, אפליקטיבי</u>**
מדיניות ובקרות נדרשות	תהליכי	הגדרת מדיניות	יישום	יישום ברמה אפליקטיבית + אפשרות הגדרת מדיניות נוספת מחמירה יותר	יישום ברמות תשתית, פלטפורמה ואפליקטיבית+ אפשרות הגדרת מדיניות נוספת מחמירה יותר
מדיניות ובקרות נדרשות	טכנולוגי	רכש כלים מרכזיים בהתקנה מרכזית	מיכון ואכיפה טכנולוגית (כלים מרכזיים או מקומיים)	מיכון ואכיפה טכנולוגית (כלים מרכזיים או מקומיים) - ברמה אפליקטיבית	מיכון ואכיפה טכנולוגית (כלים מקומיים) ברמות תשתית, פלטפורמה ואפליקטיבית
מוכנות וכ"א מיומן	תהליכי	הגדרת דרישות סף למוכנות משרדים כולל כ"א מינימלי (כישורים, הסמכות, ניסיון) הגדרת פרופילי כ"א הנגשת הדרכות והסמכות	איוש כ"א בהתאם – עבור רמות התשתית והפלטפורמה	איוש כ"א בהתאם – עבור הרמה האפליקטיבית	איוש כ"א בהתאם – ברמות תשתית, פלטפורמה ואפליקטיבית

נושא	רובד תהליכי / טכנולוגי	שותפים			
		מערך הדיגיטל	מערך הדיגיטל הלאומי ושירותים משותפים **<u>תשתית ופלטפורמה</u>**	משרד הצורך אזור נחיתה ושירותים משותפים **<u>רמה אפליקטיבית בלבד</u>**	משרד שאינו צורך אזור נחיתה ושירותים משותפים **<u>כל הרמות: תשתית, פלטפורמה, אפליקטיבי</u>**
מנגנון בחינה ואישור מערכת להגירה	תהליכי	הגדרת ומדיניות + יישום מנגנוני מחשבון סיכון, תיעוד רמת סיכון והחלטה ובקרה	אישור שירותים משותפים לפי המדיניות + מענה לשאלות משרדים לגבי צריכת השירותים המשותפים והסתמכות עליהם	אישור מערכת ע״י הנהלת המשרד לפי המדיניות (כולל הסתמכות על שירותים משותפים) - ברמה אפליקטיבית	אישור המערכת ע״י הנהלת המשרד לפי המדיניות - ברמות תשתית, פלטפורמה ואפליקטיבית
מנגנון בחינה ואישור מערכת להגירה	טכנולוגי	ראה ״ ניהול רמת הגנה (posture management)״ + הגדרת מדיניות לגבי סקירה טרום מעבר ליצור	ראה ״ ניהול רמת הגנה (posture management)״ + ביצוע סקירה טרום מעבר ליצור + תיקון ממצאים	ראה ״ ניהול רמת הגנה (posture management)״ + ביצוע סקירה טרום מעבר ליצור + תיקון ממצאים כל זאת ברמה אפליקטיבית	ראה ״ ניהול רמת הגנה (posture management)״ + ביצוע סקירה טרום מעבר ליצור + תיקון ממצאים כל זאת ברמות תשתית, פלטפורמה ואפליקטיבית
הבטחת ציות (Assurance	תהליכי	הגדרת תקן + הגדרת מסגרת בקרות אחודה (תקן ותוספות) + הגדרת שיטות assurance	עמידה בתקן + ביקורת חיצונית לתקן + קיום הבקרות	עמידה בתקן + ביקורת חיצונית לתקן + קיום הבקרות כל זאת ברמה אפליקטיבית	עמידה בתקן + ביקורת חיצונית לתקן + קיום הבקרות כל זאת ברמות תשתית, פלטפורמה ואפליקטיבית
ניהול רמת הגנה (posture manageme nt)	תהליכי	הגדרת מדיניות שימוש + הסדרת נראות (visibility) וגישה ברמת משרד ורמת גוף מרכזי + SLA לתיקון ממצאים מבוסס-סיכון	תהליך חיבור משרדים לכלי הניטור + יישום המדיניות לגבי שירותים משותפים כולל תהליך תיקון ממצאים ומעקב	יישום המדיניות לגבי המערכת כולל תהליך תיקון ממצאים ומעקב כל זאת ברמה אפליקטיבית	יישום המדיניות לגבי התשתית, הפלטפורמה והמערכת, כולל תהליך תיקון ממצאים ומעקב כל זאת ברמות תשתית, פלטפורמה ואפליקטיבית

נושא	רובד תהליכי / טכנולוגי	שותפים			
		מערך הדיגיטל	מערך הדיגיטל הלאומי ושירותים משותפים **<u>תשתית ופלטפורמה</u>**	משרד הצורך אזור נחיתה ושירותים משותפים **<u>רמה אפליקטיבית בלבד</u>**	משרד שאינו צורך אזור נחיתה ושירותים משותפים **<u>כל הרמות: תשתית, פלטפורמה, אפליקטיבי</u>**
הבטחת ציות (Assurance) + ניהול רמת הגנה (posture manageme nt)	טכנולוגי	רכש כלי posture management + רכש כלי attack surface management	יישום והנגשת ניטור ממוכן למשרדים + הגדרת מסגרת בקרות אחודה (מבוסס תקן ותוספות) בכלי + ניטור השירותים המשותפים עצמם - בעזרת הכלי מול התקן	ניטור ממוכן של המערכת - בעזרת הכלי מול התקן כל זאת ברמה אפליקטיבית	ניטור ממוכן של התשתית, הפלטפורמה והמערכת - בעזרת הכלי מול התקן כל זאת ברמות תשתית, פלטפורמה ואפליקטיבית
רציפות תפקודית והמשכיות עסקית	תהליכי	מדיניות למשרדים בחינת שירותים משותפים רלוונטיים	הגדרת נהלים בהתאם למדיניות יישום תהליכים ובקרות תרגול תקופתי	הגדרת נהלים בהתאם למדיניות יישום תהליכים ובקרות תרגול תקופתי	הגדרת נהלים בהתאם למדיניות יישום תהליכים ובקרות תרגול תקופתי
רציפות תפקודית והמשכיות עסקית	טכנולוגי		קיום המדיניות ככל שהוגדר, הנגשת שירותים משותפים רלוונטיים	קיום הדרישות בתוך ועובר העננים שבשימוש ברמה אפליקטיבית כולל המידע	קיום הדרישות בתוך ועובר העננים שבשימוש בכל הרמות – תשתית, פלטפורמה, ואפליקטיבית כולל המידע
שירותים משותפים	תהליכי	זיהוי, תיעדוף, הגדרה, תכנון, תקצוב, רכש ככל שנדרש	יישום השירותים עפ"י הנחיות מערך הדיגיטל	צריכת השירותים עפ"י הנחיות מערך הדיגיטל	קבלת אישור החרגה משימוש באזור נחיתה משותף עמידה מלאה בכל דרישות הגנת הסייבר ברמות תשתית, פלטפורמה ואפליקטיבית צריכת שירותים משותפים אחרים
מודל תפעולי ומודל אחריות משותפת	תהליכי	הגדרת מודל, תחומי אחריות ותחומי תפעול כולל כל הרמות וכולל משרדים שאינם באזור נחיתה משותף	יישום המדיניות והמשימות כספק שירותים משותפים יישום המדיניות עבור מערכות שבאחריותם, כמו כל מערכת משרד	יישום המדיניות והמשימות כבעלי מערכת אחריות וידוא קיום בקרות	יישום המדיניות ברמת תשתית, פלטפורמה ובעלי המערכת אחריות וידוא קיום בקרות

נושא	רובד תהליכי / טכנולוגי	שותפים			
		מערך הדיגיטל	מערך הדיגיטל הלאומי ושירותים משותפים **<u>תשתית ופלטפורמה</u>**	משרד הצורך אזור נחיתה ושירותים משותפים **<u>רמה אפליקטיבית בלבד</u>**	משרד שאינו צורך אזור נחיתה ושירותים משותפים **<u>כל הרמות: תשתית, פלטפורמה, אפליקטיבי</u>**
מעקב, בקרה, איתור חריגים, אכיפה	תהליכי	הגדרת מדיניות + הגדרת ויישום מנגנון בקרה ואיתור חריגים + הגדרת ויישום מנגנון אכיפה (כולל תעדוף מקצועי לרכש כלים והגדרת מנגנוני השימוש בהם)	יישום ותמיכה בדרישות המדיניות	יישום ותמיכה בדרישות המדיניות ברמה אפליקטיבית	יישום ותמיכה בדרישות המדיניות כל זאת ברמות תשתית, פלטפורמה ואפליקטיבית
מעקב, בקרה, איתור חריגים, אכיפה	טכנולוגי	הגדרת כלי נדרשים (כגון posture management) + תקצוב ורכש	יישום כלים מרכזיים ככל שנדרש חיבור השירותים המשותפים לכלים מרכזיים ככל שנדרש	חיבור המערכת לכלים מרכזיים ככל שנדרש ברמה אפליקטיבית	חיבור התשתית, פלטפורמה ומערכת לכלים מרכזיים ככל שנדרש כל זאת ברמות תשתית, פלטפורמה ואפליקטיבית
שיפור רמת בשלות של יכולת המשילות	תהליכי	הגדרת מנגנון, תדירות ומשך + מדדים והיבטים יישום המנגנון	תמיכה ביישום המנגנון ככל שיידרש תמיכה ומענה לבחינה תקופתית ככל שיידרש	תמיכה ומענה לבחינה תקופתית ככל שיידרש	תמיכה ומענה לבחינה תקופתית ככל שיידרש
שירותים מרכזיים כמו אספקת מידע מודיעיני Threat Intelligence וסיוע באירועים Incident Response	טכנולוגי	התקשרות עסקית עם ספקים לצורך מתן שירות כמענה רוחבי בתחום זה לרבות כלים, תקצוב ורכש	תמיכה ביישום המנגנון ככל שיידרש תמיכה ומענה לבחינה תקופתית ככל שיידרש	יישום ותמיכה בדרישות המדיניות ברמה אפליקטיבית	יישום ותמיכה בדרישות המדיניות כל זאת ברמות תשתית, פלטפורמה ואפליקטיבית

<u>נספח 2 - פעילויות ניהול סיכוני הסייבר בשלבי המיגרציה השונים</u>

שלב במודל הליך המיגרציה לענן	פעילויות נדרשות לניהול אפקטיבי של סיכוני סייבר בענן
היערכות והכנה	1. הכרת והבנת המודל התפעולי וחלוקת האחריות בין המשרד לגופי ממשלה. 2. הכרת והבנת אזור הנחיתה המשותף ושירותים משותפים אחרים. 3. הבנת מודל האחריות המשותפת בין ספק הענן למשרד ומופעיו השונים בהתאם למודלי השירות, ארכיטקטורות אפשריות, ושירותים ספציפיים של ספקי הענן. 4. הכרת והבנת מדיניות הממשלה למעבר לענן בכלל ומדיניות הגנת הסייבר בענן בפרט. 5. הכרת והבנת תהליך ההגירה, צמתי קבלת החלטות ואופן קבלתן, פעילויות נדרשות בכלל ובהיבטי סייבר בפרט. 6. הבנת יכולות הגנת הסייבר בענן הנדרשות מהמשרד כולל תפקידים, כישורים וידע, תהליכים וכלים – לצורך ההגירה עצמה ולצורך השימוש בענן לאחר ההגירה.
הערכת התאמה לענן	1. סיווג המערכת והערכת הסיכון תוך מיקוד בנזק (Impact) כולל סיווג המידע, קריטיות המערכת, רגולציה, חשיפות וסיכונים ייחודיים ובסבירות להתממשות הסיכון (Likelihood). 2. בחינת התאמת המערכת לענן (ככל שרלוונטי, הבהרת התאמת המערכת לענן זמני בחו״ל או ספק SaaS בחו״ל, בשונה מהתאמה לאזור ענן בישראל)
תכנון הליך המיגרציה	1. ניתוח סיכונים פרטני למערכת בכלל ובהתאם לאסטרטגית ההגירה בפרט (למשל: SaaS מול IaaS; הגירה של המערכת כפי שהיא או התאמת הארכיטקטורה לענן; שימוש בקונטיינרים) - וזאת היות ומתאר הסיכונים, הבקרות הנדרשות והבקרות הזמינות ישתנו בהתאם. 2. בחירת בקרות נדרשות ודרישות הגנת סייבר פרטניות למערכת. 3. הבהרת תחומי האחריות על הבקרות (ספק הענן, שירותים משותפים מרכזיים, המשרד, התאמות ובקרות מפצות) 4. הגדרת תכנון מפורט של יישום הבקרות. 5. השלמת יכולות חסרות בהתאמה. 6. הקצאת משאבים ובעלי תפקידים לקיום התהליכים והבקרות שהוגדרו.
ביצוע הליך המיגרציה	1. וידוא יישום או הפעלת הבקרות ע״י ספק הענן, ובהתאמה, באחריות הספק לוודא זאת מול שרשרת האספקה שלו (למשל ספק SaaS לגבי ספק ה-IaaS עליו הוא מתבסס). 2. יישום בקרות בצד המשרד. 3. וידוא או יישום התאמות נדרשות – קביעת פרמטרים, תצורה ובקרות מפצות.
מוכנות לשימוש ותחילת שימוש	1. אישור השימוש. 2. ניטור שוטף של קיום ותפעול הבקרות בתחומי האחריות השונים.

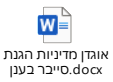
נספח 3 - התאמות נדרשות עבור הענן במסגרת ניהול הסיכונים

סוג פעילות	שלב	התאמות נדרשות עבור הענן במסגרת ניהול הסיכונים
הערכה	סיווג	סיווג המערכת והערכת הסיכון תוך מיקוד בנזק (Impact) – כולל סיווג המידע, קריטיות המערכת, רגולציה, חשיפות וסיכונים ייחודיים, ובסבירות להתממשותו (Likelihood). בחינת סיכונים ייחודיים/ מוגברים בענן מבחינת חשיפה, הסתברות ונזק (לעומת ניהול המערכת on premise)
הערכה	זיהוי בקרות	• זיהוי בקרות נדרשות בהינתן סיווג המערכת והמידע וניתוח הסיכון. • הגדרה ברורה של תחומי האחריות: בקרות באחריות ספק הענן, בקרות באחריות המשרד (צרכן הענן) והתאמות נדרשות (כגון קביעת פרמטרים ע"י הצרכן בבקרות ושירותים שמנגיש הספק, או בקרות מפצות מעבר למה שספק הענן מציע). מומלץ לבצע זאת בד בבד עם בחירת מודל שירות הענן, הספק וגישת ההגירה (מבין האפשרויות הזמינות, וכמוגדר בהנחיות הממשלה להגירה לענן) בשל ההזנה וההשפעה ההדדית.
טיפול	יישום בקרות	יישום בקרות והתאמות באחריות המשרד. (כגון קביעת פרמטרים ע"י הצרכן בבקרות ושירותים שמנגיש הספק, או בקרות מפצות מעבר למה שספק הענן מציע)
טיפול	הערכת הבקרות	ביצוע הערכת בקרות בכל תחומי האחריות ובהתאם להם (ספק, צרכן, התאמות)
טיפול	אישור שימוש	ביצוע הפעילויות כמוגדר במסגרת הכללית לניהול סיכוני סייבר
בקרה	ניטור	ניטור שוטף של קיום ותפעול הבקרות בתחומי האחריות השונים הערכה תקופתית ושילוב בקרות רציפות וחידוש אישור המערכת, ספק הענן/שירות ותצורת השימוש, והבקרות שיושמו להגנת המערכת

11. נספחים תומכים (חיצוניים)

מצורף בקובץ נפרד

- נספח א – מדיניות הגנת סייבר בענן לגופים ממשלתיים (אוגדן מסמכי מדיניות הגנת הסייבר הממשלתית לענן)



- נספח ג – REGULATION AND STANDARDS BENCHMARK OVERVIEW