מערך הדיגיטל הלאומי
نظام الديجيتال الوطني
Israel National Digital Agency

הנחיות מערך הדיגיטל הלאומי

שם ההנחיה: מדיניות ניהול הרשאות ובקרת גישה		
פרק ראשי: טכנולוגיות		מספר הנחיה:
פרק משני: מחשוב ענן- CCoE	מס' גרסה: 1.0	בתוקף מ-01.06.2024

1. מטרת המסמך

1.1. מסמך זה מהווה מדיניות למערכת ההרשאות הממשלתית עבור משרדי הממשלה ויחידות הסמך.

1.2. מערכת הרשאות ממשלתית הינה תשתית לאומית שתינתן בשירות למשרדי הממשלה, ותוגדר בשירות חובה לניהול זהויות והרשאות גישה לכל מערכות המידע והתשתיות של משרדי הממשלה ויחידות הסמך. מערכת הרשאות ממשלתית תיתן למשרד יכולות נראות (Visibility) ומשילות (Governance) גבוהות יותר של תהליך בקרת הגישה, תוך עמידה בתאימות אחידה. מערכת זו תנהל ברמה המשרדית את הרשאות העובד למערכות מידע ולתשתיות המשרד.

2. קהל היעד

2.1. מנהלים במערך הדיגיטל הלאומי.

2.2. מנהלי היחידות מונחות מערך הדיגיטל במשרדים.

3. מונחים והגדרות

ראה מילון מונחי תקשוב

בהנחיה זו נדגיש את המונחים הבאים:

3.1. ניהול זהויות דיגיטליות (Identity and Access Management) – תהליך של ניהול ואבטחת זהויות מקוונות של משתמשים הכולל יצירה, אימות והגנה על הזהויות הדיגיטליות.

3.2. ספק זהות (IDP- Identity Provider) – מערכת שמספקת שירותי אימות זהות עבור משתמשים. מערכת זו מאפשרת למשתמשים להשתמש באותו שם משתמש וסיסמה כדי להתחבר למספר שירותים שונים.

3.3. Tenant– ארגון שמשתש בשירותי ענן. הארגון מקבל גישה למשאבים ייעודיים של ספק הענן תוך שימוש בסביבה מבודדת משאר ה-Tenants.

3.4. עיקרון הרשאות מינימליות (Least Privilege) – עיקרון אבטחה לפיו כל משתמש מקבל את ההרשאות המינימליות הדרושות לו. עיקרון זה מפחית את הסיכון של גישה לא מורשית למידע ולמשאבים ומגביל את הנזק שעלול להיגרם כתוצאה מפריצה.

4. כללי

4.1. סעיף 4 להחלטת ממשלה 231 בנושא קידום המעבר הממשלתי לענן ציבורי מיום 1.8.2021 (להלן: ההחלטה) מטיל על מערך הדיגיטל הלאומי את האחריות להקים תשתית רוחבית בענן הציבורי לניהול זהויות דיגיטליות (Identity and Access Management). סעיף 5 להחלטה קובע את השימוש בתשתית הרוחבית כחובה לכלל משרדי הממשלה ויחידות הסמך, אשר אינם רשאים לפתח או לרכוש שירותים מקבילים, אלא באישור ראש מערך הדיגיטל הלאומי. מערכות תמ"ק יקבלו מענה לפי הנחיות שייקבעו בהמשך.

המוצר הזוכה במכרז המרכזי מוגדר כתשתית רוחבית. בהתאם להחלטת הממשלה, מערך הדיגיטל יקבע מדיניות רוחבית בנוגע למבנה הנתונים, התהליכים וההפרדות על מנת לאפשר לכלל משרדי הממשלה ויחידות הסמך לעשות שימוש נכון בתשתית המרכזית, תוך יישום שירות עצמי למשרדים לניהול מחזור חיים מלא של ישויות משרדיות.

בנוסף למסמך זה יופצו שני מסמכים נוספים שישלימו את מדיניות מערכת ההרשאות הממשלתית:

- מסמך אבטחת מידע לתשתית מערכת ההרשאות הממשלתית שישקף את מדיניות יה"ב ומס"ל לגופי תמ"ק ולתשתית המוצר עצמו וכן את מדיניות ההרשאות עבור משתמשים בעלי הרשאות גבוהות.
- מסמך מודל הפעלה למערכת ההרשאות הממשלתית.

4.2. בהתאם להוראות סעיף 5 להחלטת ממשלה 231 מיום 1.8.21, טרם ביצוע הזמנה של מוצרים או שירותים בתחום ה- IDP בענן, על ידי מזמינים המונחים על ידי מערך הדיגיטל הלאומי, פירוט הגופים הדורשים את אישור מערך הדיגיטל הלאומי מצ"ב בנספח א') ניתן לפנות ליחידת המעבר לנימבוס (CCoE) במערך הדיגיטל הלאומי באמצעות פורטל נימבוס או בכתובת דוא"ל: NimbusCCoE@digital.gov.il.

4.3. בהתאם להוראות סעיף 3.ב.3 להחלטת הממשלה 1700 מיום 17.4.24, כלל הגופים למעט משרד הביטחון וצה"ל, יטמיעו ויעשו שימוש במוצרים ושירותים בתחום ה- IAM בענן בהתאם למדיניות והנחיות התפעול אשר יפורסמו על ידי מערך הדיגיטל הלאומי בפורטל נימבוס בכתובת (הכניסה לפורטל עם כרטיס חכם בלבד): https://scportal.govextra.gov.il/national-digital-agency/cloud-me-in/home-page/

5. יתרונות מערכת הרשאות ממשלתית כתשתית רוחבית

מערכת אחידה לניהול הרשאות תאפשר הקמת מערכות חוצות ממשלה, תוך מינוף יכולות הענן לצורך שיתוף משאבים והרשאות גישה למערכות מידע וזהויות. המדיניות הממשלתית שתוטמע בתשתית המרכזית תאפשר משילות והחלת מדיניות אחידה על כל החשבונות המשרדיים (Tenants).

השימוש במערכת ההרשאות הממשלתית יאפשר למשרדים את היתרונות הבאים:

5.1. יתרונות בהיבט טכנולוגי:

- הענקת זהות אחודה לספקים שצריכים גישה למספר משרדים.
- יצירת מנגנון פשוט למתן או להורדה של הרשאות למשתמש ברמת המשרד.
- ממשקי API משותפים בין משרדיים.
- התממשקות לסביבות On-prem – תמיכה בעבודה עם מערכות ניהול זהויות מקומיות (On-prem) ובהתחברות ב-SSO (Single Sign On) עם שרתי הממשלה המקומיים (On prem) עד להגירתם המלאה לענן.

- הזדהות - המערכת מאפשרת לעובדי מדינה, נותני שירות ויועצים חיצוניים לבצע הזדהות מול משרד אחד או יותר.
- יכולת ניהול זהויות מרכזית – תמיכה בניהול מרכזי ועצמאי, למשל ביצירה ובניהול מרכזיים של זהויות וקבוצות לכל משרד על ידי יצירת Organizational Unit (OU) משרדי.
- יכולות גיבוי, שחזור והעברת נתונים - תמיכה בגיבוי ובשחזור נתונים ללא תלות בתשתית ספק הענן הממשלתי, כולל מפתחות הצפנה לגיבויים הנדרשים, ויכולות העברת נתוני המערכת למערכות אחרות.

5.2. יתרונות בהיבט אבטחת מידע:

- פורטל מרכזי לשימוש עצמי עבור משרדי ממשלה ויחידות סמך (Self Service).
- הקמה וניהול זהויות באמצעות תבניות ותהליכי אוטומציה.
- יכולת תגובה מרכזית לאירועי סייבר באמצעות יכולות מובנות במערכת.
- יכולת ניטור מרכזי של מערכת הרשאות ע"י ה-SOC הממשלתי, והחלת חוקים רוחביים והתראות לכל הממשלה.
- תשתית מרכזית למערכות שונות, כגון מערכות קולבורציה, ניהול משימות ועוד.
- יכולת אכיפת מדיניות ממיקום מרכזי על ידי מערך הדיגיטל.
- קישור אחד למערכת ההזדהות הלאומית.

5.3. יתרונות בהיבט עסקי:

- בשילוב עם תהליכים של סיווג מידע ושינוי הרגולציה בשיתופי מידע בין משרדים ולגורמי חוץ, ניתן יהיה לשפר משמעותית את כל שיתוף המידע הממשלתי מתהליך של חודשים עד שנה, לתהליך שלוקח ימים ספורים. כמו כן, על ידי שימוש באמצעי זה יהיה ניתן להגדיר עבור כל משתמש ממשלתי מזוהה את רמת הרגישות של המידע אותו הוא רשאי לקבל ובמקביל את רמת הסיווג של כל מידע – כך שהעברות המידע יהיו לגורמים הרשאים לכך.
- ללא תשתית מרכזית, ייווצר קושי משמעותי בתהליכי חיבור בין המשרדים כאשר יתווספו פתרונות קולבורציה ושיתוף מסמכים.
- יצירת ספר כתובות ממשלתי אחד.
- יכולת לבנות פתרונות רוחביים המזהים את המשתמשים ברמה בין משרדית (ייצור קבוצות הרשאות רוחביות לממשלה), כגון מערכות קולבורציה, ניהול משימות.
- זמינות - צריכת המערכת בתצורת תוכנה כשירות (SaaS) ובזמינות מתמשכת בתצורת High Availability.
- היברידיות - תמיכה בתצורת ה-Multi Cloud הממשלתית.

6. תפיסת ההפעלה

במסגרת המכרז תקבע מערכת הרשאות אשר תשמש את הממשלה כמוצר בלעדי ומרכזי. מערך הדיגיטל הלאומי יבנה תהליכים מרכזיים בתשתית המוצר עבור הממשלה בהתאם למדיניות הממשלתית שתוגדר על ידי גורמי ההנחיה. תהליך זה יכלול מספר שלבים שעיקרם:

- הגדרת החלוקה של המוצר לאזורים עבור כל משרד (Tenants) ואת תצורות החיבור של משרדי הממשלה לאזורים אלה על מנת לסנכרן את המשתמשים שלהם ולנהל את מחזור חיי הישויות הללו בעצמם.
- מתן מענה לאבטחת מערכת ההרשאות הממשלתית ולחבר אותה ל-SOC הממשלתי.
- קביעת מדיניות לגבי אופן השימוש במערכת והסייגים (Guardrails) שלה.

6.1. לצורך מימוש התשתית יידרשו תהליכים של מעבר מהמערכות הקיימות בכל משרד וקישור של מערכות המשרד והיישומים השונים למערכת הזהויות.

6.2. תהליך ההגירה של המערכות והתממשקות למערכות הקיימות צפוי להימשך מספר שנים. לפיכך, לאחר גיבוש מפת הדרכים המשרדית לענן, ובמסגרת מפת הדרכים הממשלתית לענן אשר ייעשו במהלך שנת 2024, ייבחן מתווה ממשלתי לניהול מהלך זה ע"י צוות ייעודי בראשות יחידת הגנה בסייבר (יה"ב) ביחד עם צוות המוצר במערך הדיגיטל הלאומי ומערך הסייבר הלאומי.

6.3. התשתית תוקם על ידי צוות ייעודי שיוקם במערך הדיגיטל הלאומי שיוגדר למטרה זו. תפקידי הצוות:

- ניהול פעילות המוצר מול הספק הזוכה
- הגדרת מדיניות רוחבית
- קביעת תהליכי סנכרון ויצירת מנגנונים לחיבור המשרדים
- ליווי תהליך הטמעה (כמוגדר בסעיף 6) במשרדים
- סיוע למשרדים

6.4. במערכת ההרשאות הממשלתית יוטמעו שני סוגים של משתמשים:

6.4.1. משתמש קצה מסוג בן אדם (Human)

- זיהוי חד ערכי של משתמש אנושי, אזרח מדינת ישראל, יתבצע מול מערכת ההזדהות הלאומית ובמערכת החדשה יוגדרו רק ההרשאות של הישות במשרדים השונים.
- משתמש אנושי שאינו אזרח מדינת ישראל וזהותו לא מנוהלת במערכת ההזדהות הלאומית (לדוגמא: יועצים זרים מחו"ל, שאמורים לקבל הרשאה לפרק זמן מוגבל) יוגדרו ישירות במערכת ה-ההרשאות הממשלתית.
- לאחר זיהוי תקין המערכת תבצע בדיקת הרשאות לביצוע פעולות.

6.4.2. משתמש מסוג מכונה (Service Account)

- משתמש זה יוגדר במערכת ניהול הרשאות.
- יוגדרו הרשאות גישה למשתמש.

6.5. מימוש מערכת ההרשאות תבוצע בסביבת הבדיקות לפני העברת המערכת לסביבת ייצור.

7. שילוב יישום ושירותי הרשאות

לטובת יצירת אחידות ונוחות ליישום מערכת הרשאות ממשלתית, יבצע כל משרד, בהתאם לצרכיו, שילוב יישומים ושירותי זהות מגוונים, בהתבסס על אפשרויות ותרחישי השימוש הקיימים והמפורטים בסעיף זה להלן:

- ניהול המערכת וההרשאות יבוצע מאזור ייעודי למשרד הממשלתי או ליחידת הסמך, על פי הצורך.
- שילוב עם מערכות ניהול זהויות צד שלישי בהתאם לדרישה.
- אינטגרציה למערכת אימות רב שלבית (MFA-Multi Factor Authentication) מבוססת יישומים בהתאם לצורך (עבור משתמשי קצה).
- קישור של מערכת ההרשאות למערכות המשרד והיישומים השונים שלו באמצעות Single Sign On (SSO).
- המשרדים יוכלו לעדכן את פרופיל המשתמש באמצעות פורטל מרכזי וכן לאפס סיסמאות ולשחזר סיסמה באופן עצמאי בצורה מאובטחת.
- לצורך המעבר, למערכת ההרשאות הממשלתית תהיה יכולת לסנכרן רשומות פרטניות ממערכת ניהול הזהויות המשרדית (Active Directory) למערכת ההרשאות הממשלתית.
- למשרד תהיה יכולת גריעה או הקפאה של משתמשים ממערכת ההרשאות עקב חוסר שימוש, והפקת דוחות לטובת איתור משתמשים "רדומים" שלא בשימוש במשך תקופה מוגדרת, בהתאם להנחיית יה"ב 5.12.
- המערכת תאפשר איחוד זהויות כפולות או נתונים כפולים (כגון משתמש העובד בשני משרדי ממשלה שונים) בהתאם להרשאות המשרד.
- מערכת ההרשאות הממשלתית תומכת בשימוש בתבניות מוגדרות מראש לפרטי זהויות (Configurable Schema Interfaces) ותתמוך בנתוני זהויות ייחודיות כגון מספר דרכון.
- המוצר יאפשר אינטגרציה עם מוצר הזהות הלאומית בתהליך זיהוי המשתמש.

8. אבטחת תהליך ניהול הרשאות

הטמעת מערכת הרשאות ממשלתית מחייבת עמידה בעקרונות אבטחת מידע לניהול זהויות, המבוססת על הנחיות יה"ב, כמפורט מטה. הנחיות לגופי תמ"ק יפורסמו בהמשך.

- הגדרת מדיניות אביפה מרכזית על ידי מערך הדיגיטל הלאומי.
- ביצוע שימוש באימות רב שלבי (MFA) או הזדהות ביומטרית, תוך הגדרת מדיניות אביפה.
- במערכת ההרשאות תהיה הגדרה, בהתאם להנחיות הכלליות של הממשלה, של מנגנון נעילת חשבונות בצורה מרכזית במקרי חירום.
- הנפקת תעודות עבור מערכת ההרשאות תתבצע על בסיס שרתי תעודות (CA - Certificate Authority) ידועים מראש.
- מערכת ההרשאות תעשה שימוש ביכולות אנליטיות מבוססות משתמש (UBA – User Behavior Analytics), כגון זיהוי פעולות זיוף, התנהגות משתמש חשודה ועוד.
- לצורך ניטור מערך הזהויות, יוגדרו ניטור והתממשקות למערכות ניטור SIEM ע"י ה-SOC הממשלתי, ויוגדרו חוקים רלוונטיים. במקביל, תוגדר שמירה של לוגים (Logs) אודות פעולות מערכת, ניהול הזהויות, והגישה למידע במערכת, במבנה לוגים סטנדרטי לתקופה שתוגדר על ידי הממשלה.
- מערכת ההרשאות תשולב באוטומציה של תהליכים ותהיה חלק מהתגובה בעת אירועי סייבר SOAR, והפעלת Playbooks בטיפול באירועי סייבר חריגים.
- לצורך תחקור מעמיק וזיהוי מגמות, מערכת ההרשאות הממשלתית תתמוך בהגדרות להפקת דוחות רלוונטיים, בדגש על שינויים לא תקינים ברמת ההרשאות ופערים קיימים אל מול המלצות יצרן (Configuration Management).

- המערכת תנהל את הרשאות המשתמשים במערכות השונות. ניהול הרשאות והגבלתן ייעשה על פי עיקרון הרשאות מינימליות (Least Privilege) במערכת.
- על המשרד להגדיר מדיניות ניהול סיסמאות, תוך אביפה של מורכבות הסיסמא (Password Complexity) על פי הנחיית יה"ב הרלוונטית. בניהול סיסמאות תהיה יכולת אביפת מורכבת - סיסמה ברמת משתמש בודד וברמת מנהל מערכת.
- לצורך שמירה על פרטיות מקסימלית, יופעלו יכולות ערבול נתוני הזהויות.
- על המשרד המשתמש במערכת ניהול הרשאות ממשלתית להגביל מתן ההרשאות על בסיס זמני השימוש הנחוצים (Conditional Access & JIT) ולהגביל הרשאות לאורחים.
- מערכת ההרשאות מאפשרת תהליך פיתוח (DevOps) בצורה מאובטחת. תהליך ניהול הזהויות בשרשרת הפיתוח יבוצע על ידי שימוש בתפקידים (Roles) ייעודיים ומתן הרשאות לתפקידים אלו בלבד- ללא מתן הרשאות באופן ישיר למשתמש משרדי.

9. עקרונות ההטמעה במערך הדיגיטל ובמשרדי הממשלה

מערך הדיגיטל יוודא הטמעת והיכרות עם המדיניות בכל משרדי הממשלה.

בניית מתווה הטמעה שיורכב מהפרטים הבאים:

- היכרות עם מוצר.
- תוכנית הכשרה לשימוש במוצר.
- תוכנית מעבר ממוצר ניהול זהויות קיים למערכת ההרשאות הממשלתית.
- היערכות לשלב היברידי בו יהיה סנכרון בין שני המוצרים (הישן והחדש).
- תהליך הגירת מערכות להתממשקות עם מערכת ניהול ההרשאות הממשלתית.

ההטמעה תיעשה באופן עצמאי ע"י המשרדים יחד עם האינטגרטור על פי נוהל חיבור למערכת שייקבע.

10. חלוקת אחריות

לצורך מימוש מערכת הרשאות ממשלתית, להלן מודל חלוקת אחריות, אשר יעודכן עם קביעת המדיניות הפרטנית.

	משרד ממשלתי	מערך הדיגיטל
יישום וניהול מערכת הרשאות ממשלתית התשתית (IAM)		
הגדרת מדיניות ממשלתית ברמת התשתית (כולל מדיניות ניהול סיסמאות)		
חיבור ל SOC הממשלתי		
הכשרה והטמעה		
הגדרה ותפעול חשבונות משתמשים		
הגדרות קבוצות עבודה (Security Roles)		

	משרד ממשלתי	מערך הדיגיטל
הפקת וניהול דוחות לטובת איתור משתמשים "רדומים" שלא בשימוש במשך תקופה מוגדרת		
סנכרון רשומות ספציפיות ממערכת ניהול הזהויות המשרדית (Active Directory) למערכת ניהול ההרשאות הממשלתית		
תוכנית הגירה משרדית של מערכות מול מערכת ההזדהות הלאומית		

11. מסמכים ישימים

החלטת הממשלה 231 מתאריך 1.8.2021

12. גרסאות ההנחיה

מס'	סטאטוס	מהות שינוי	סעיפים שהושפעו	בתוקף מ-	נכתב ע"י	אושר ע"י
0.1	מאושר לפרסום	גרסה ראשונה		1.6.2024	יערה גלבוע אייל	שירה לב עמי

13. נספח א- רשימת גופים

להלן רשימת הגופים החייבים באישור מערך הדיגיטל הלאומי לשם ביצוע הזמנה:

1. רשות מקרקעי ישראל - רמ"י
2. נציבות שירות המדינה
3. רשות התחרות
4. הרשות הממשלתית למים ולביוב
5. רשות האוכלוסין וההגירה
6. השירות המטאורולוגי
7. הרבנות הראשית לישראל
8. בתי הדין הרבניים
9. הנהלת בתי המשפט
10. הרשות להגנת הצרכן ולסחר הוגן
11. המכון הגיאולוגי לישראל
12. רשות המסים בישראל
13. רשות האכיפה והגבייה
14. מינהל התכנון
15. מערך הסייבר הלאומי
16. כבאות והצלה לישראל
17. הלשכה המרכזית לסטטיסטיקה
18. משרד האנרגיה והתשתיות
19. משרד התקשורת
20. המשרד לשוויון חברתי וקידום מעמד האישה
21. משרד החקלאות ופיתוח הכפר
22. משרד העלייה והקליטה
23. משרד הבריאות
24. משרד הכלכלה והתעשייה
25. משרד הבינוי והשיכון
26. המשרד להגנת הסביבה
27. משרד התיירות
28. המשרד לשירותי דת
29. משרד העבודה
30. משרד הפנים
31. משרד הנגב, הגליל והחוסן הלאומי
32. משרד הביטחון
33. משרד הרווחה והביטחון החברתי
34. משרד התרבות והספורט
35. משרד החוץ
36. משרד המשפטים
37. משרד האוצר
38. משרד התפוצות והמאבק באנטישמיות

39. משרד ראש הממשלה
40. משרד החדשנות, המדע והטכנולוגיה
41. משרד התחבורה והבטיחות בדרכים
42. משרד החינוך
43. המשרד לביטחון לאומי
44. משרד המורשת
45. משרד ירושלים ומסורת ישראל
46. המשרד לשיתוף פעולה אזורי
47. משרד ההתיישבות והמשימות הלאומיות
48. המשרד לעניינים אסטרטגיים
49. שירות התעסוקה הישראלי
50. המוסד לביטוח לאומי