

דוח מבקר המדינה | סייבר ומערכות מידע | התשפ"ג-2022



רשות המיסים בישראל

---

**הגנת סייבר  
והמשכיות עסקית  
ביחידת שירות  
עיבודים ממוכנים  
ברשות המיסים**





## הגנת סייבר והמשכיות עסקית ביחידת שירות עיבודים ממוכנים ברשות המיסים

### רקע

שירות עיבודים ממוכנים (שע"ם) הוא גוף המשמש מערך המחשוב של רשות המיסים בישראל ונותן לה שירותי מחשוב לצורך גבייה ואכיפה, ליצירת הרתעה ראויה ולמיצוי זכויותיהם של הנישומים. שע"ם משרת כ-1.3 מיליון "לקוחות": חברות, תאגידים מסוגים אחרים, עצמאים, בעלי שליטה, שכירים, מקבלי מענקי עבודה, שכירים המבצעים תיאומי מס והחזרי מס, 6,000 העובדים של רשות המיסים, 13,000 משרדי מייצגים ו-7,000 עורכי דין. שע"ם מנהל מאות פרויקטים בכל שנה, החל בפרויקטים לביצוע מידי וכלה בפרויקטים שביצועם נמשך שנים מספר. שע"ם מחזיק במערכתיו מידע על אזרחים, נישומים, עוסקים וגופים נוספים.

החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 קובע את תחומי הסמכויות והאחריות לאבטחה פיזית, לאבטחת מידע ולאבטחת מערכות מחשוב חיוניות של גופים ציבוריים שונים, לרבות גופי ממשלה וגופים בבעלות פרטית. החוק מגדיר מערכות ממוחשבות חיוניות כ"מערכות ממוחשבות שנקבעו כחיוניות על ידי הגוף שהסמיכה לכך הממשלה".

בשנת 2010 החליטה ועדת היגוי עליונה כי שע"ם יכלל בתוספת השנייה והחמישית לחוק הסדרת הביטחון. בהתאם לכך, מערך הסייבר הלאומי הוסמך לתת הנחיות מקצועיות בתחום אבטחת מערכות מחשוב חיוניות לשע"ם.



## נתוני מפתח

### חלק

מעובדי שע"ם הנדרשים לסיווג אינם בעלי סיווג נדרש

### 1.3 מיליון

מקבלי שירות משע"ם: חברות, תאגידים, עצמאיים, שכירים ועוד


### 2014

השנה בה החלה הכנת תוכנית המשכיות עסקית בשע"ם, תהליך שטרם הסתיים

### 11

מספר ממצאי מבדק החוסן שביצע יועץ חיצוני מטעמו של משרד מבקר המדינה

## פעולות הביקורת

בחודשים נובמבר 2021 - פברואר 2022 בדק משרד מבקר המדינה את אבטחת המידע והגנת הסייבר בשע"ם. הביקורת נעשתה בשע"ם, ובדיקות השלמה נעשו במערך הסייבר הלאומי. 

במסגרת הביקורת נבדקו היבטים מסוימים בהגנת סייבר, נעשתה בדיקת חוסן למערכת התומכת בתהליך עסקי ברשות המיסים (מערכת א'), ונבדקה היערכות שע"ם להמשכיות הפעילות העסקית ולהתאוששות מאסון.

הדוח שבנדון הומצא לראש הממשלה ביום 31.7.2022 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה.

מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב], ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתיאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא הונחו על שולחן הכנסת ולא יפורסמו.

ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאתו האמור לעיל.



## תמונת המצב העולה מן הביקורת

**תפקידי ועדת היגוי לנושא התמ"ק** - עלה כי תפקידי הוועדה הוגדרו בכתב המינוי באופן כללי, והם לא פורטו כנדרש בהנחיות הרגולטוריות. עלה כי דיוני הוועדה אינם עוסקים בפעולות שתנקוט הוועדה בהתאם לתפקידיה, כפי שנדרש בהנחיות.

**מיפוי תהליכים ונכסי מידע** - על פי ההנחיות הרגולטוריות, על הגוף למפות את נכסי המידע והגישות אליהם, כדי להתאים תוכנית אבטחה. עלו פערים במיפוי התהליכים ונכסי המידע שבוצע בשע"ם והוא אינו עונה במלואו על דרישות ההנחיות הרגולטוריות.

**פערים בנוהלי שע"ם** - בביקורת עלה כי במספר נהלים בשע"ם נמצאו אי התאמות להנחיות הרגולטוריות, בין היתר, בנושא ממשק העבודה מול מערך הסייבר הלאומי.

- **ניהול שינויים** - לא נמצאה בנוהל הרלוונטי התייחסות לצורך לעדכן את הגורם הרלוונטי ולשתפו בנייתוח הסיכונים וההשפעות הצפויות של השינויים כנדרש בהנחיות.

- **נוהל טיפול באירועי אבטחת מידע** - נמצא כי בשע"ם קיים נוהל אך הוא אינו עוסק בחובה לדווח לגורם הרלוונטי ולצורך לשלבו בתחקור האירוע. בנוסף חסרה התייחסות רלוונטית לתחום מסוים הנדרש בהנחיות.

**ריכוז מידע בדבר שרשרת אספקה** - עלו פערים בדבר המידע שנאסף על ידי אגף אבטחת מידע בשע"ם בנוגע לשרשרת האספקה. כמו כן, לא נעשה שימוש במודול שרשרת אספקה במערכת הייעודית שפיתח מערך הסייבר הלאומי.

**חולשה בשרת מסוים** - עלו פערים בבקרה על השרת המסוים.

**סיווג נדרש** - הביקורת העלתה כי קיימים פערים בין רמת הסיווג הנדרשת בהתאם לתפקידיהם של חלק מהעובדים בשע"ם לבין רמת הסיווג שלהם בפועל.

### בדיקת חוסן מטעם משרד מבקר המדינה על מערכת א'

מערכת זו תומכת בתהליך עסקי ברשות המיסים. במהלך הבדיקה הועלו ממצאים אשר מסכנים מהבחינה העסקית את המידע ואת מוניטין הארגון.

### היערכות להמשכיות עסקית והתאוששות מאסון

**הסדרת פעילות האגף** - בנובמבר 2016 החליט מנהל שע"ם כי לצורך הקמת אגף איכות והמשכיות עסקית יתוכנן מבנה ארגוני לאגף בסיוע יועצים. נציבות שירות המדינה התנתה את אישור האגף באישור נחיצותו מטעם רשות התקשוב הממשלתי. עלה כי האגף פועל מסוף שנת 2016, אף שהנציבות לא אישרה את שינוי המבנה הארגוני. הגדרות התפקיד של עובדי האגף הן הגדרות תפקידיהם הקודמים, והם מועסקים בהתאם לתקנים שהוקצו לאגפים אחרים. בעקבות זאת סמכות האגף ותפקידיו אינם מוסדרים.



**תוכנית התאוששות מאסון** - תוכנית התאוששות מאסון כוללת תוכנית להתאוששות המערך הטכנולוגי, תהליך הפעלת מצב החירום, תהליך החזרה ממצב החירום לשיגרה, תרגילי החירום ומדדים עיקריים להתאוששות:






Return Point Objective (RPO) - כמות המידע שאבד בהתרחש אסון.

Return Time Objective (RTO) - משך הזמן המרבי מרגע קבלת ההחלטה עד להפעלת אתר החירום.

נמצאו פערים בנוגע להשלמת תוכנית התאוששות מאסון.

**תוכנית להמשכיות עסקית** - נמצאו פערים בתהליך גיבוש תוכנית להמשכיות עסקית ובהשלמתה.

## עיקרי המלצות הביקורת

- מומלץ כי שע"ם יתקן את הליקויים שנמצאו במיפוי התהליכים ונכסי המידע שנערך. 
- מומלץ כי שע"ם יעדכן את נהליו באופן שיכללו את כל הפעולות הנדרשות בהתאם להנחיות הרגולטוריות. 
- מומלץ כי שע"ם ישתמש במערכת הייעודית שפיתח מערך הסייבר הלאומי לבחינת שרשרת האספקה. 
- מומלץ כי שע"ם יפעל לכך שרמת הסיווג של כלל העובדים בשע"ם תותאם לתפקידיהם. 
- מומלץ כי שע"ם יבחן את הממצאים שהועלו במבדק החוסן שנערך מטעם משרד המבקר המדינה ויתקן את הליקויים שהועלו בדוח זה. 



## סיכום

שע"ם הוא גוף ה-IT של רשות המיסים, וככזה הוא מפתח מערכות מידע עבודה, מתחזק מערכות קיימות ומחזיק במידע. יש חשיבות גדולה לרמה גבוהה של הגנת סייבר בשע"ם וכן לתפקוד מלא של שע"ם בעתות משבר והתאוששות מהירה מאסון.

ממצאי הביקורת מעלים כי על שע"ם לפעול לשיפור הגנת הסייבר על מערכתיו.

מומלץ כי שע"ם יפעל בהקדם לתיקון הליקויים שהועלו בדוח זה תוך בחינת יישום המלצות הדוח.







## הגנת סייבר והמשכיות עסקית ביחידת שירות עיבודים ממוכנים ברשות המיסים

### מבוא

שירות עיבודים ממוכנים (להלן - שע"ם) הוא גוף המשמש מערך המחשוב של רשות המיסים בישראל ונותן לה שירותי מחשוב לצורך גבייה ואכיפה, ליצירת הרתעה ראויה ולמיצוי זכויותיהם של הנישומים. שע"ם משרת כ-1.3 מיליון "לקוחות": חברות, תאגידים מסוגים אחרים, עצמאים, בעלי שליטה, שכירים, מקבלי מענקי עבודה, שכירים המבצעים תיאומי מס והחזרי מס, 6,000 העובדים של רשות המיסים, 13,000 משרדי מייצגים ו-7,000 עורכי דין. שע"ם מנהל מאות פרויקטים בכל שנה, החל בפרויקטים לביצוע מידי וכלה בפרויקטים שביצועם נמשך שנים מספר. שע"ם מחזיק במערכתיו מידע על אזרחים, נישומים, עוסקים וגופים נוספים.

אלו תפקידי שע"ם: הספקת מערכות מחשוב ושירותי מחשוב המשמשים תשתית לגביית מס אמת; הענקת שירות המעמיד את הלקוח במרכז; שימוש בטכנולוגיות חדשות כדי לממש את מטרותיה של רשות המיסים; פיתוח ושימור של ההון האנושי, הערכי והמקצועי על פי החזון של רשות המיסים, החותרת להיות גוף חדשני ויוזם הפועל ביעילות ובאפקטיביות.

החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - חוק הסדרת הביטחון או החוק), קובע את תחומי הסמכויות והאחריות לאבטחה פיזית, לאבטחת מידע ולאבטחת מערכות מחשוב חיוניות של גופים ציבוריים שונים, לרבות גופי ממשלה וגופים בבעלות פרטית. החוק מגדיר מערכות ממוחשבות חיוניות כ"מערכות ממוחשבות שנקבעו כחיוניות על ידי הגוף שהסמיכה לכך הממשלה"<sup>1</sup>. בחוק נקבעו, בין היתר, סמכויותיו של ממונה הביטחון וכפיפותו המקצועית לקצין מוסמך - נציג השב"כ, המשטרה או הרשות הלאומית להגנת הסייבר בהתאם לגוף; סמכותו של קצין מוסמך לתת הנחיות מקצועיות לאחראי לאבטחת מערכות ממוחשבות חיוניות בכל הנוגע לפעולות אבטחה בגופים אשר נכללו בתוספת השנייה או החמישית לחוק (להלן - גופי תמ"ק<sup>2</sup>). עד אוגוסט 2016 היה הקצין המוסמך לעניין אבטחת מערכות מידע לגופי תמ"ק נציג שב"כ ולאחר מכן - נציג מערך הסייבר הלאומי (להלן - המערך).

על פי ההנחיות הרגולטוריות (להלן - ההנחיות), גוף שיש לו מערכת קריטית אשר פגיעה בה עלולה להביא לידי נזק, בהתאם לתבחיני נזק שנקבעו, נדרש להנחותו. העמידה בתבחינים נבחנת על ידי ועדת היגוי, ואם החליטה הוועדה כי הגוף המונחה עומד בתבחינים, יחל תהליך שבסופו יחול על הגוף חוק הסדרת הביטחון. גופי תמ"ק הם גופים אשר נכללו בתוספת השנייה או החמישית לחוק הסדרת הביטחון, ובהם רשות המיסים.

1 סעיף 1 בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998.

2 תשתיות מחשוב קריטיות.



חוק הסדרת הביטחון מקנה לקצין מוסמך את הסמכות לתת הנחיות לגופי תמ"ק. בחוק נקבע כי נציג המערך ישמש קצין מוסמך, ובסמכותו לתת הנחיות מקצועיות לאחראי לאבטחת מערכות ממוחשבות חיוניות בכל הנוגע לפעולות אבטחה.

מערכת מחשוב קריטית היא מערכת אשר פגיעה בה עלולה לגרום לנזקים שהוגדרו בהנחיות. גוף שיש לו מערכת מחשוב קריטית ייחשב גוף תמ"ק<sup>3</sup>.

הנחיית גופי תמ"ק היא תהליך מורכב המתבצע באופן שוטף תוך היזון חוזר. בשלב הראשון עובדי המערך לומדים את תהליכי העבודה ואת מרכיבי המערכות בגוף, בוחנים את פוטנציאל הנזק ואת הדפ"אות לתקיפת סייבר של הגוף או המערכת הקריטית, מגדירים עם הגוף המונחה את הנכסים להגנה ומגבשים תמונת מצב של יכולות ההגנה, וכפועל יוצא מכך מגדירים את משימת ההגנה. הפעילות השוטפת כוללת המלצה על יעדי הגנה וגיבוש יעדים אלה בהתאם להנחיות הרגולטוריות, ביצוע סקר למיפוי פערי ההגנה, הכנת תוכנית לצמצום הפערים והטמעת המענה האבטחתי. תוכנית הטמעת המענה האבטחתי נחלקת למספר שלבים.

## פעולות הביקורת

בחודשים נובמבר 2021 - פברואר 2022 בדק משרד מבקר המדינה את אבטחת המידע והגנת הסייבר בשע"ם. הביקורת נעשתה בשע"ם, ובדיקות השלמה נעשו במערך הסייבר הלאומי.

במסגרת הביקורת נבדקו היבטים מסוימים בהגנת סייבר, נעשתה בדיקת חוסן למערכת התומכת בתהליך עסקי ברשות המיסים (להלן - מערכת א'), ונבדקה היערכות שע"ם להמשכיות הפעילות העסקית להתאוששות מאסון.

הדוח שבנדון הומצא לראש הממשלה ביום 31.7.2022 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה.

מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב] ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתיאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא הונחו על שולחן הכנסת ולא יפורסמו.

ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאתו האמור לעיל.

## הגנת סייבר בשע"ם

### ועדת היגוי לנושא התמ"ק

על פי ההנחיות הרגולטוריות. גוף מונחה נדרש להקים ועדת היגוי לנושא התמ"ק. בהנחיות נקבעו בין היתר תחומי האחריות של ועדת ההיגוי ותדירות התכנסותה.

3 אם הוא נכלל בתוספת השנייה או החמישית לחוק.



בכתב המינוי של ועדת ההיגוי להגנת הסייבר בשע"ם ממרץ 2019 הוגדרו תפקידי הוועדה כלהלן: אישור מדיניות וכללים מנחים באבטחת מידע וסייבר, אישור תוכנית עבודה ומעקב אחר ביצועה, הנחיה של שע"ם וקידום היערכותו להגנת סייבר בעיתות שגרה וחירום. כמו כן נקבע כי ועדת ההיגוי תארגן ותנחה את הפעילות ותפקח עליה, על פי ההנחיות הרגולטוריות. בכתב המינוי נרשם כי ועדת ההיגוי תתכנס אחת לחודש.

הואיל ותפקידי הוועדה בכתב המינוי הוגדרו באופן כללי ולא פורטו, צוות הביקורת בחן את תפקידי הוועדה כפי שעלו בדיון של ועדת ההיגוי. בדיון זה הוחלט כי הוועדה תתכנס אחת לחודש, ולאחר מכן במרווחים גדולים יותר.

בכתב המינוי מינואר 2022 הוגדרו תפקידי הוועדה כלהלן: "לדון בהתקדמות רגולציות סייבר שונות; הצגת תוכניות עבודת סייבר שנתית ואישורה; הצגת אירועי סייבר וקבלת החלטות באשר לביצוע תיקוני ממצאים; קבלת החלטות באשר למחלוקות בין הנושאים העסקיים לנושאי הסייבר (ניהול סיכונים); אישור משאבי עבודה לכלל שע"ם בנושאי סייבר". כמו כן נקבע כי ועדת ההיגוי תתכנס אחת לחודש למשך שעת עבודה אחת.

עלה כי הגם שתפקידי הוועדה הוגדרו בכתב המינוי, הם הוגדרו באופן כללי ולא פורטו כנדרש בהנחיות הרגולטוריות.

עוד נמצא כי, כפי שעולה מפרוטוקולים של דיוני הוועדה, הדיונים עוסקים בעיקר בתוכנית העבודה של אגף אבטחת מידע, בליווי פרויקטים ובטיפול בתקלות, וכי הדיונים אינם עוסקים בפעולות שתנקוט הוועדה בהתאם לתפקידי הוועדה כפי שנדרש בהנחיות הרגולטוריות.

משרד מבקר המדינה ממליץ לשע"ם לעדכן את כתב המינוי של ועדת ההיגוי באופן שיכלול את תפקידי הוועדה כנדרש בהנחיות הרגולטוריות, וכן הוא ממליץ לשע"ם לפעול ליישום תפקידי הוועדה.

רשות המיסים מסרה בהבהרתה מ-19.6.22 כי כתב המינוי יתוקן על פי המלצת המבקר.

בכתב המינוי ממרץ 2019 נרשם כי ועדת ההיגוי תתכנס אחת לחודש, אך בפרוטוקול של הדיון הראשון של הוועדה משנת 2019 נקבע, כאמור, כי "הוועדה תתכנס אחת לחודש ולאחר מכן במרווחים גדולים יותר".

עלה כי בשנת 2019 התכנסה ועדת ההיגוי בהתאם להנחיות הרגולטוריות. עם זאת מספר ההתכנסויות אינו עולה בקנה אחד עם כתב המינוי של הוועדה ממרץ 2019.

מומלץ לשקול לעדכן את כתב המינוי, בהתאם לצורך ולמספר ההתכנסויות בפועל.

## מיפוי תהליכים ונכסי מידע

על פי ההנחיות הרגולטוריות, על הגוף למפות את נכסי המידע והגישות אליהם, כדי להתאים תוכנית אבטחה.



עלו פערים במיפוי התהליכים ונכסי המידע שבוצע בשע"ם, והוא אינו עונה במלואו על דרישות ההנחיות הרגולטוריות.

רשות המיסים מסרה בתשובתה מ-8.6.2022 (להלן - תשובת רשות המיסים) כי בתחילת שנת 2022 היא נקטה בצעדים לשיפור המצב.

בהנחיות הרגולטוריות נקבע כי יש לתכנן תוכנית עבודה להתאמת המענה האבטחתי לגוף המונחה. תוכנית העבודה אמורה לכלול את הפעולות הנדרשות לביצוע בהתבסס על ממצאי המיפוי שנעשה.

נמצא כי בשע"ם הוכנה תוכנית עבודה ומעקב אחר הפערים בין ההנחיות לנעשה בפועל. עם זאת, בשל פערים במיפוי התהליכים ונכסי המידע הנדרש, תוכנית זו נותנת מענה חלקי. עוד עלה כי הגנה על רשת א' כמקשה אחת, ללא ניתוח התהליכים הפרטניים והבחנה ביניהם, יוצרת מערך הגנה רחב מהנדרש, והדבר עלול ליצור קשיים תפעוליים בשע"ם.

מערך הסייבר מסר במהלך הביקורת כי הוא מודע לפערים במיפוי התהליכים ונכסי המידע, ולכן הנחיותיו לשע"ם כוללות מענה פרטני ורחב יותר מאשר בגופים אחרים, אשר מפצה על הפער.

משרד מבקר המדינה ממליץ כי שע"ם יתקן את הליקויים שנמצאו במיפוי התהליכים ונכסי המידע שנערך.

## סקר סיכונים

בהנחיות הרגולטוריות נקבע כי יש לבצע סקר סיכונים לתהליכים מסוימים אחת לתקופה. על בסיס הסקר יש להכין תוכנית עבודה להתאמת המענה האבטחתי.

נמצא כי בוצע בשע"ם סקר סיכונים כולל במגוון תחומים, ביניהם גם אבטחת מידע. הסקר התבסס על סדנאות מנהלים אשר העלו סיכונים משמעותיים הנוגעים לשע"ם. סקר זה עסק בהיבטים מסוימים הקשורים לאבטחת מידע אך לא עסק בהיבטים אחרים הקשורים בנושא זה.

עלה כי סקר הסיכונים בשע"ם ביצע בתחום אבטחת המידע, אינו תואם את ההנחיות הרגולטוריות בדבר ביצוע סקר הסיכונים. עוד נמצא כי שע"ם אינו מפקח על הטיפול בממצאי הסקר שנערך.

משרד מבקר המדינה ממליץ כי שע"ם יבצע סקר סיכונים בהתאם להנחיות הרגולטוריות.

בביקורת שביצע מערך הסייבר בשע"ם בחודשים ינואר - פברואר 2018 נבחנו היבטי הגנת הסייבר ברשת ב'. רשת זו הוקמה בעקבות ביקורת משנת 2016, שערך רגולטור מסוים.

בביקורת של מערך הסייבר עלו בין היתר סיכונים בתהליכי העבודה.



בחודשים נובמבר - דצמבר 2019 מערך הסייבר ביצע ביקורת בנוגע לרשת א' בשע"ם. בביקורת עלו סיכונים שונים.

נמצא כי בשע"ם לא התקיים תהליך של מעקב אחר הטיפול בליקויים שהועלו בביקורת המערך שהוזכרו לעיל.

רשות המיסים מסרה ביום 20.7.22 כי בוצע מעקב על רשת ב' וכי בהמשך עלו תקלות נוספות ברשת, ולכן המשך התהליך היה בהתכתבויות מול מערך הסייבר. עוד נמסר כי לא בוצע מעקב סדור לטיפול בממצאי בקרת המערך בנושא רשת א' הואיל ו"שע"ם נכנס לתקופה מסיבית של יישום החזר מענקים לנפגעי הקורונה ובכלל התמודדות עם עבודה מרחוק".

## נוהלי אבטחת מידע בשע"ם

שע"ם פועל כגוף IT<sup>4</sup> זה שנים רבות. במהלך השנים נכתבו נהלים, בין היתר בתחומי אבטחת המידע, והם מתעדכנים מפעם לפעם. בשע"ם התבצע עדכון נהלים בשנת 2016, בין היתר כחלק מדרישות ההסמכה של תקני אבטחת המידע. בשנת 2018 החל שע"ם בעדכון העמידה בדרישות תקני אבטחת המידע, בין היתר בעדכון נהלים. זאת ועוד, בשל היות שע"ם גוף תמ"ק, הוחלט לעדכן את הנהלים גם על פי דרישות ההנחיות הרגולטוריות נוסף על דרישות תקני אבטחת המידע. הנהלים עודכנו שוב בשנים 2020 - 2021, בסיוע חברת ייעוץ. בתהליך זה בוטלו נהלים שאינם תקפים ואוחדו נהלים כפולים.

## תהליך פיתוח או שינוי מערכת

על פי ההנחיות, על הגוף המונחה לעדכן את הגורם הרלוונטי לפני יישום כל שינוי משמעותי הנוגע לתהליכים קריטיים. הגוף המונחה נדרש לכתוב נוהל העוסק בסיכונים ובהשפעות הצפויות של יישום השינוי. על פי ההנחיות, הגורם הרלוונטי יהיה מעורב בניתוח הסיכונים ובתהליך התאמת המענה.

הביקורת העלתה כי אף שנושא ניהול השינויים נכלל בנוהל העוסק בהיבטי אבטחת מידע בכל שלבי הפרויקט, הנוהל אינו עוסק בצורך לעדכן את הגורם הרלוונטי בניתוח הסיכונים ובהשפעות הצפויות של יישום השינויים כנדרש בהנחיות.

משרד מבקר המדינה ממליץ לשע"ם לעדכן את הנוהל באופן שיכלול את כל הפעולות הנדרשות בהתאם להנחיות הרגולטוריות.

רשות המיסים מסרה בתשובתה כי אגף המשכיות עסקית בשע"ם יכתוב נוהל אשר יכלול את כל הפעולות הנדרשות בהתאם להנחיות הרגולטוריות.



## נוהל טיפול באירוע אבטחת מידע

בהנחיות נדרש להגדיר את ההיערכות לטיפול באירועים חריגים ואת תהליך הטיפול בהם. על פי ההנחיות טיפול יתבצע רק לאחר עדכון הגורם הרלוונטי.

הביקורת העלתה כי בשע"ם קיים נוהל תגובה לאירועי אבטחת מידע וסייבר מפברואר 2020, אך הנוהל אינו עוסק בחובה לדווח לגורם הרלוונטי על אירועים אלה, ולצורך לשלבו בתחקור האירוע. כמו כן חסרה התייחסות רלוונטית לתחום מסוים הנדרש בהנחיות. משרד מבקר המדינה ממליץ לשע"ם לעדכן את נוהל תגובה לאירוע אבטחת מידע וסייבר, באופן שיכלול את כל הפעולות הנדרשות בהתאם להנחיות.

## נוהל עבודה בנושא שרשרת האספקה

בהנחיות הרגולטוריות מפורטות דרישות אשר על הגוף המונחה לפעול לפיהן, בין היתר בנושאים הנוגעים לעבודה עם ספק חיצוני.

הביקורת העלתה כי הנוהל בשע"ם אינו כולל את כל הדרישות שנקבעו בהנחיות. משרד מבקר המדינה ממליץ לשע"ם לעדכן את נוהל שרשרת האספקה באופן שיכלול את כל הנדרש בהנחיות.

## אבטחת המידע בשע"ם

### שרשרת האספקה

כאמור, בהנחיות הרגולטוריות יש הנחיה לפעילות מול ספקים חיצוניים על מנת להתגונן מפני איומי תוקף באמצעות שרשרת האספקה.

הביקורת העלתה פערים בדבר המידע שנאסף על ידי אגף אבטחת מידע בשע"ם בנוגע לשרשרת האספקה.

מערך הסייבר הלאומי פיתח מערכת ממוחשבת המאפשרת לכל ארגון בישראל לבדוק את רמת הגנת הסייבר ואת מידת עמידתו של הארגון בתקנים מקומיים ובין-לאומיים באופן אנונימי, דינמי ופשוט. במערכת זו נכלל, בין היתר, מודול שרשרת אספקה ובו, בין היתר, שאלון ספקים, שאותו ממלא הספק. השאלון מאפשר לארגונים הערכה של הסיכונים והבנה של רמת ההגנה של הספק, ובד בבד הוא מאפשר לספקים להבין מהן הדרישות והבקורות הנדרשות על מנת שיוכלו לעמוד ברמת ההגנה הנאותה.

בביקורת עלה כי לא נעשה שימוש במודול שרשרת אספקה במערכת הייעודית.



רשות המיסים מסרה בתשובתה כי נושא זה לא קודם בשל תיעדוף הטיפול בנושאים דחופים יותר.

מומלץ כי שע"ם ישתמש במערכת הייעודית שפיתח מערך הסייבר הלאומי לבחינת שרשרת האספקה.

## ניהול הרשאות

שע"ם נותן שירות לאלפי משתמשי קצה, עובדי מס הכנסה, מייצגים ממשרדי רואי חשבון, יועצי מס ואזרחים. בשרתי שע"ם מאוחסן מידע המכיל פרטים בדבר הכנסות של נישומים ופרטים אישיים. מידע זה עלול להיות מנוצל לרעה במגוון רחב של דרכים. שע"ם הגדיר לכל קבוצת משתמשים את ההרשאות המתאימות לה, ונדרש שהמידע יהיה נגיש רק למי שרשאי להיחשף אליו, וכי הרשאות הגישה יתעדכנו כל העת בהתאם לסטטוס המשתמשים.

בהנחיות הרגולטוריות יש התייחסות לנושא ההרשאות, ונקבע בהן כי יש לגבש נהלים המתייחסים לנושאים אלו.

בנובמבר 2021 הוכן דוח הביקורת הפנימית בנושא "הרשאות גישה בשע"ם". במסגרת תגובת שע"ם על דוח הביקורת הפנימית צוין כי נושא ההרשאות נסקר ומפוקח גם במסגרת עמידה בתקנים ורגולציות, וגם במסגרת תוכנית העבודה השנתית של צוות אבטחת מידע המבצע סקירת הרשאות עיתית.

הביקורת העלתה כי שע"ם משתמש במערכת ממוחשבת לניהול הרשאות.

## פיתוח מאובטח

שע"ם מספק כאמור שירותי מחשוב, ומועסקים בו מפתחים הכותבים קוד למערכות קיימות ואף למערכות חדשות. כתיבת קוד מאובטח משדרגת את רמת אבטחת המערכת. בהנחיות הרגולטוריות יש הנחיה בנושא פיתוח מאובטח.

עלה כי הטמעת מדיניות פיתוח מאובטח קודמה במידה רבה, אך אינה מלאה.

רשות המיסים מסרה בתשובתה כי בכונת שע"ם לפעול לתיקון הליקוי.

## מבדקי חדירה

על פי ההנחיות הרגולטוריות, יש לבצע מבדק חדירה לרכיבי המערכת הקריטית אחת לתקופה. מטרת המבדק לבחון את איתנות המערכת הקריטית.

בשל ריבוי המערכות שע"ם מתקשה לבצע מבדקי חדירה לכלל המערכות אחת לתקופה. בשל כך הנחה המערך לבצע פעילות מסוימת כבקרה מפצה.



הביקורת העלתה כי שע"ם ביצע את הפעילות בחלק מן המערכות אולם עלו פערים בהשלמת הבקורות המפצות. משרד מבקר המדינה ממליץ להכין תוכנית לסגירת הפער.

רשות המיסים מסרה בתשובתה כי בשנת 2022 פעלה באמצעים אחרים לצורך גישור על הפער במבדקי החדירה.

## **ביקורת רגולטור מסוים**

בשנת 2016 בוצעה ביקורת מקיפה של רגולטור מסוים בשע"ם בביקורת נבחנו כמה תחומים בכמה מן המערכות בשע"ם.

### **1. חולשה בשרת מסוים**

בביקורת הרגולטור עלו פערים.

הביקורת העלתה פערים בבקרה על השרת. משרד מבקר המדינה ממליץ לשע"ם לפעול לכך שהבקרה על מערכתיה תהיה מלאה.

### **2. סיווג נדרש**

בביקורת רגולטור מסוים שנערכה לפני מספר שנים עלו פערים בניהול ובבקרה על רשימת העובדים בשע"ם הנדרשים בסיווג.

הביקורת העלתה כי קיימים פערים בין רמת הסיווג הביטחוני הנדרשת בהתאם לתפקידיהם של חלק מהעובדים לבין רמת הסיווג שלהם בפועל. משרד מבקר המדינה ממליץ לשע"ם לפעול לכך שרמת הסיווג הנדרשת של כלל העובדים בשע"ם תותאם לתפקידיהם.

רשות המיסים מסרה בתשובתה כי צוות הביטחון בשע"ם יפעל למתן הכשר לעובדים בהתאם לרמת הסיווג הנדרשת לתפקידם.

### **3. פריסת רכיב**

בביקורת הרגולטור המסוים שנערכה לפני מספר שנים עלו פערים בפריסת רכיב מחשובי מסוים.

הביקורת העלתה כי ניתן מענה לפער שהעלתה ביקורת הרגולטור המסוים לפני מספר שנים.





## בדיקת חוסן - מערכת א'

בפברואר 2022 ביצע משרד מבקר המדינה בדיקת חוסן אפליקטיבית, בסיוע יועץ חיצוני. הבדיקה נעשתה במערכת א' התומכת בתהליך עסקי ברשות המיסים. מטרת הבדיקה הייתה למדוד את רמת האבטחה של המערכת תוך שימת דגש על ההיבטים האלה: החוסן האפליקטיבי של המערכת<sup>5</sup>, איתור פערים בין רמת אבטחת המידע של המערכת ובין רמת אבטחת המידע המיטבית האפשרית ואיתור של חולשות ומפגעים אפליקטיביים קיימים.

הבדיקה נעשתה במספר היבטים ובהם: מניעת השבתת פעילות המערכת, מניעת ביצוע פעולות לא רצויות, יישום מדיניות, עדכונים ושמירה מידע.

בבדיקה נבחנה כאמור רמת מוגנות אבטחת המידע ברמת האפליקציה, ובסביבת בדיקות, ומכאן שמנגנוני ההגנה ההיקפיים של שע"ם לא נבחנו ולא הופעלו בבדיקה זו. זאת כדי לבחון את חוסן המערכת בהיעדר מנגנוני הגנה אלו או בהנחה שתוקף יכול להתגבר על הגנות אלו. מנגנונים אלו יכולים לעכב או למנוע חלק מהתקיפות המועלות בבדיקה זו.

במבדק החדירה שביצע היועץ החיצוני מטעמו של משרד מבקר המדינה הועלו ממצאים אשר מסכנים מהבחינה עסקית את המידע ואת מוניטין הארגון.

משרד מבקר המדינה ממליץ לשע"ם לבחון ממצאים אלו, וכן לבחון את ההמלצות לתיקון הליקויים שהועלו על מנת להעלות את רמת החוסן האפליקטיבי של מערכת א'.

רשות המיסים מסרה בתשובתה כי היא מקבלת את המלצת משרד מבקר המדינה בנושא בדיקת החוסן האפליקטיבית, וכי היא פועלת לתיקון הליקויים שנמצאו בה.

## המשכיות עסקית והתאוששות מאסון

### היערכות להמשכיות עסקית והתאוששות מאסון

המשכיות עסקית (BCP - Business Continuity Program) היא דוקטרינת ניהול של הפעולות שארגון נדרש לבצע כדי להבטיח שהפונקציות העסקיות החיוניות יהיו זמינות ללקוחות, לספקים, לגופי האסדרה ולגופים אחרים בעלי עניין בארגון. תוכנית המשכיות עסקית אינה נוגעת בפעולות ההצלה הראשוניות המתבצעות בהתרחש אירוע חירום, אלא בהתכוננות ובהתארגנות להשגת יכולת תפקוד ולהתאוששות מהירה לאחר האירוע.

על פי הגדרת רשות התקשוב הממשלתי (להלן - רשות התקשוב)<sup>6</sup>, תוכנית המשכיות עסקית ותפקודית (הנקראת גם "מערכת ניהול המשכיות עסקית") היא "תוכנית פעולה מקיפה, הקובעת נהלים ומערכות הדרושים כדי לשמר את המשכיות פעילות המשרד במצב חירום ולשקמה, במידת הצורך".

5 חוסן אפליקטיבי הוא מוגנות אבטחת המידע ברמת האפליקציה.

6 בהחלטת הממשלה 135 מיוני 2021 נקבע כי יוקם מערך הדיגיטל הלאומי, אשר יכלול את רשות התקשוב הממשלתי ואת המימון הלאומי "ישראל דיגיטלית" ואליו יועברו סמכויותיהם.



השירותים והתהליכים העסקיים של משרדי הממשלה מושתתים על טכנולוגיות מידע דיגיטליות. השבתה של מערך המחשוב כולו או של חלקו עלולה להסב נזק של ממש לתחום העסקי, לתחום הכלכלי ולתדמית של המשרד. הנחיות רשות התקשוב מחייבות את אגפי תקשוב של משרדי ממשלה. הרשות פרסמה הנחיות בנושא שנועדו להדריך את משרדי הממשלה בנושא.

בשנת 2016<sup>7</sup> פרסם ראש רשות התקשוב את הנחיה מס' 5.2 במסגרת הנחיות היחידה להגנת הסייבר בממשלה (יה"ב), שכותרתה "הנחיית מסגרת להגנת הסייבר בממשלה". בהנחיה פורטו עקרונות מנחים להבטחת המשכיות העסקית באגפי המחשוב: הגדרת מערכות ותהליכים חיוניים לפעילות הגוף והגדרת פרק הזמן הדרוש להתאוששותם, זיהוי תרחישי ייחוס והערכת השפעותיהם, הגדרת בעלי סמכות להסדרה, כתיבת תוכנית להמשכיות עסקית על רכיביה השונים והסדרת מערך בקרה.

בעקבות משבר הקורונה פורסמה הנחייתו של ראש רשות התקשוב הממשלתית בנושא "היערכות להמשכיות עסקית ותפקודית במצב חירום" (להלן - ההנחיה), התקפה מ-18.11.20. ההנחיה מרחיבה ומעמיקה את ההנחיה הקודמת. היא קובעת תהליכי עבודה שנועדו להכין ארגונים לתרחישי חירום באופן שיספר את השרידות של מערכות המידע החיוניות ויאפשר להן להתאושש במהירות מקריסה. ההנחיה עוסקת במסגרת העבודה, בנושאים שיש לכלול בתוכנית המשכיות העסקית, בהטמעת התוכנית ובתרגולה, בהספקת כלי תקשורת ונגישות, בתיעוד כל המסמכים הרלוונטיים, בהסדרת שיטות עבודה בשעת חירום, בהסדרת העבודה עם הספקים בשעת חירום ובמשילות.

לעניין זה נחשב שע"ם לאגף התקשוב של רשות המיסים היות שהוא הגוף האחראי לשירותי המחשוב בה.

## פעילות האגף לאיכות ולהמשכיות עסקית

### הסדרת פעילות האגף

בנובמבר 2016 החליט מנהל שע"ם דאז כי לצורך הקמת אגף איכות והמשכיות עסקית (להלן - האגף) יתוכנן מבנה ארגוני לאגף בסיוע יועצים. בישיבה בראשות מנהל שע"ם דאז ב-20.12.16 דווח על הרכב צוות האגף: מנהל ושבעה עובדים, ונקבעו תחומי עיסוקם - המשכיות עסקית, עמידה בתקינת איכות והטמעתה, ניהול סיכונים וניהול תהליכי הפקת לקחים (להלן - תחכימים).

על פי חוק שירות המדינה (מינויים), התשי"ט-1959 הסמכות לשינויי תקינה בשירות המדינה, ובכללם קביעת מבנים ארגוניים, נתונה בידי נציב שירות המדינה. אגף בכיר משרדי הממשלה ויחידות הסמך בנציבות שירות המדינה (להלן - הנציבות) אחראי בין השאר להמליץ לנציב שירות המדינה על שינויי תקינה ועל שינויים מבניים שיאפשרו ליחידה ממשלתית להשיג את יעדיה ומטרותיה. קביעת מבנה ארגוני כוללת קביעת אופיון ומהותן של המשרות באותה יחידה, קביעת דירוגם המתאים של העובדים מבין הדירוגים הקיימים בשירות המדינה, עריכה ואישור של תיאור התפקיד המתאר את המשרה אשר על פיו יפורסם מכרז לאיושה כמתחייב מחוק המינויים, וכל הליך אחר המתחייב על פי החוק והתקנות.

7 ההנחיה עודכנה בשנת 2017.



נציבות שירות המדינה התנתה את אישור האגף באישור נחיצותו מטעם רשות התקשוב. בפגישה שהתקיימה בספטמבר 2018 בעניין זה בין מנהל האגף לבין נציג רשות התקשוב לא ראה נציג הרשות הצדקה להקמת האגף במבנה שהוצע, משום שלכאורה מדובר במשימות חד-פעמיות שאינן מצדיקות מבנה ועובדים כפי שהוצג לפניו.

בביקורת עלה כי האגף פועל מסוף שנת 2016 אף שהנציבות לא אישרה את שינוי המבנה הארגוני. הגדרות התפקיד של עובדי האגף הן הגדרות תפקידיהם הקודמות, והם מועסקים בתקנים שהוקצו לאגפים אחרים. בעקבות זאת סמכות האגף ותפקידיו אינם מוסדרים. במהלך השנים עזבו את האגף ארבעה עובדים, ולא ניתן היה לגייס עובדים חדשים בשל היעדר תקנים.

מצב שבו אגף איכות והמשכיות עסקית פועל חמש שנים ללא הסדרת תקן כנדרש אינו תקין. על ש"ע"ם לוודא כי יוסדר תחום המשכיות העסקית בהתאם להוראות הנציבות.

בתשובת נציבות שירות המדינה מ-25.5.22 נמסר כי בתקופה זו מגובש שינוי ארגוני בש"ע"ם, אך עדיין לא הוגשה בקשה לשינוי והמבנה הארגוני החדש לא הוצג לה. במסגרת השינוי הארגוני נדרש להסדיר, בין היתר, את המבנה הארגוני של אגף המשכיות עסקית.

### מינוי ממונה והגדרת תפקידו

בהנחיה מוטלת חובה על אגף התקשוב של משרד ממשלתי כדלקמן: "האגף ימנה אחראי המשכיות עסקית ותפקודית ויגדיר את תחומי אחריותו וסמכויותיו, שיכללו, לכל הפחות, ויודאו קיום תוכנית להמשכיות עסקית ותפקודית, עדכונה כנדרש, הצפת נושאים לדיון בפני הנהלת האגף והנהלת המשרד, לרבות בנושא האפקטיביות של תהליכי הטמעה ותרגול שנערכו באגף".

בביקורת עלה כי האחראי בפועל, שהוא ראש אגף איכות והמשכיות עסקית, לא קיבל כתב מינוי לתפקיד, ולא הוגדרו בכתב תחומי אחריותו וסמכותו.

על ש"ע"ם למנות בכתב את האחראי להמשכיות עסקית ולהגדיר בכתב את סמכויותיו ואת תפקידיו.

### ביצוע תוכנית העבודה בתחום המשכיות עסקית

תוכנית עבודה היא הכלי של גופים להוציא לפועל את מטרותיהם. לפני כל שנת תקציב מתכנן ש"ע"ם תוכנית עבודה; לכל אגף נקבעות המשימות שעליו לבצע בשנה זו ונקבעים המשאבים שיוקצו לשם כך. תוכנית העבודה המלאה של האגף משקפת את תפקידיו בתחומים אלה: המשכיות עסקית, ניהול סיכונים, עמידה בתקינת איכות והטמעתה וניהול תהליכי הפקת לקחים (תחכימים).

מהנתונים עולה כי בשנים 2019-2021 היה ניצול חלקי של ימי העבודה המתוכננים.

האגף ציין כי תוכנית העבודה שלו לשנת 2021 לא בוצעה מאחר שהתהליכים בש"ע"ם לא הושלמו ולא עודכנו במלואם.



מומלץ כי האגף והנהלת שע"ם יפעלו במשותף למימוש תוכנית העבודה והמשאבים שהוקצו לנושא המשכיות העסקית על בסיס שנתי.

## תוכנית המשכיות עסקית

על פי ההנחיה, יש לקבוע את תוכנית המשכיות העסקית והתפקודית של המשרד בהתאם להנחיות הגורמים המוסמכים לעניין תפקוד במצבי חירום. במסגרת התוכנית להמשכיות עסקית יש לבחון את היבטי התקשוב.

כהיערכות לביצוע התוכנית יש לנקוט פעולות אלה:

1. מיפוי של תרחישי ייחוס;
  2. ניתוח הסיכונים הנוצרים עקב התממשות תרחישי הייחוס (BIA<sup>8</sup>). בשלב זה נדרש הגוף לזהות ולמפות את התהליכים החיוניים ואת השירותים החיוניים ולנתח את ההשפעות העסקיות והתפקודיות של הפסקת הפעילויות במצב חירום או של הפרעה להן. כמו כן, בשלב זה יש להגדיר עבור כל אחד מהשירותים החיוניים את פרק הזמן שהמשרד יכול לפעול באופן תקין כשהשירות אינו פעיל ומהו היקף המידע שהמשרד יכול לאבד בלא שייגרם לו נזק ממשי;
  3. הגדרת יעדי השירות למצב החירום: הגדרת השירותים שתיתן יחידת המחשוב בעת חירום כדי לתמוך בפעילות החיונית של המשרד.
- פיתוח התוכנית להמשכיות עסקית מאפשר בין היתר לממש את יעדי השירות בעת חירום. על התוכנית לכלול הנחיות לפעולה בתחומים אלה:
1. כוח אדם - דרכים ושיטות לתפקוד באמצעות כוח אדם מצומצם, לרבות הגדרת כוח האדם החיוני והכנת תוכנית גיבוי;
  2. אתרי עבודה - היערכות מראש לחלופות למקום העבודה - באתרים שונים או בבית העובד;
  3. טכנולוגיה
- א. זיהוי ומיפוי של רכיבי הטכנולוגיה הנדרשים לתמיכה בהמשכיות העסקית, לרבות תשתיות ומשאבים, ממשקים לגורמים חיצוניים, תשתיות לאבטחת מידע ותשתיות אחרות;
- ב. קביעת נהלים לגיבוי ולאחזור של נתונים בהתאם ליעדי השירות הנדרשים;
  - ג. תוכנית התאוששות מאסון (DRP<sup>9</sup>) - תוכנית להתאוששות מערך המחשוב;
  4. הטמעה ותרגול באמצעות כתיבת נהלים, הדרכה ותרגול בעת שגרה;

8. Business Impact Analysis - BIA

9. Disaster Recovery Plan - DRP



5. ספקים וקבלנים בשעת חירום - הסדרת קבלת השירותים הנדרשים לרשות בשעת חירום אשר תלויים בספקים או בקבלנים.

### פעילות שע"ם בתחום ההמשכיות העסקית עד להקמת האגף

בשנת 2014, לפני הקמתו של אגף איכות והמשכיות עסקית, החל שע"ם לנקוט פעולות להסדרת ההמשכיות העסקית בסיוע יועצים חיצוניים. באותה שנה הוכן אוגדן היערכות לחירום (להלן - פק"ל שע"ם). הפק"ל כלל מיפוי של יחידות שע"ם ושל תחומי אחריותן, סקירת תרחישי ייחוס, ניתוח השפעת תרחישי הייחוס על תפקוד האגפים בשע"ם והתוויית צעדים לכתיבת תוכנית המשכיות עסקית.

בשנת 2015 החל שע"ם בתהליך התעדה של תקן איכות ישראלי. תקן זה קובע מסגרת לניהול הרציפות העסקית וכולל מפרט דרישות ליצירת מערכת ניהול מתועדת. היועצים חילקו את תהליך ההתעדה לתקן ל-16 שלבים. עד אמצע שנת 2015 בוצעו תשעה שלבים.

בשנת 2016 הכינו היועצים מדריך ליישום תוכנית המשכיות עסקית בשע"ם, המסביר כיצד מנוהלת התוכנית להמשכיות עסקית וכיצד יש למלא את דרישות התקן בארגון. כמו כן נכתבה טיוטה חלקית לתוכנית ההמשכיות העסקית. בסיום עבודת היועצים בשנת 2017 עדיין לא הושלמה התוכנית.

עלה כי תהליך ההתעדה של שע"ם לתקן האיכות הישראלי לא הושלם, על אף המשאבים הרבים שהושקעו בו.

בשנת 2019 הכין האגף, בסיוע יועץ רשות המיסים להמשכיות עסקית, מסמך יזום לתוכנית המשכיות עסקית בעת חירום בשע"ם. המסמך נועד להגדיר את השלבים הנדרשים לביצוע תוכנית ההמשכיות העסקית, והוא כולל מסגרת מושגית לתחום ההמשכיות העסקית, תרחישי ייחוס בסביבת הפעילות של שע"ם וכן פעולת שיש לנקוט כדי לקדם את התחום:

1. מיפוי של המערכות ושל השירותים העיקריים;
2. מיפוי בעלי העניין, צורכיהם וציפיותיהם;
3. מיפוי האיומים והסיכונים;
4. הכנת תוכנית ניהול סיכונים;
5. בדיקת ההשפעות של איומים וסיכונים על רציפות השירותים;
6. תכנון תגובה על האיומים והסיכונים או למניעתם וקביעת סידורים לחידוש הפעילויות הללו בעת אירוע;
7. קביעת נהלים שלהם יזדקק שע"ם כדי ליישם את הדרישות.



## עדכון אוגדן היערכות לחירום (פק"ל שע"ם)

תוכנית התאוששות מאסון (Disaster Recovery Plan - DRP) היא תוכנית לחידוש הפעילות של הטכנולוגיות ושל מערכות מידע. תוכנית זו היא רכיב מרכזי בתוכנית ההמשכיות העסקית והתפקודית. בהנחיית רשות התקשוב נקבע בעניין זה כי "האגף [מחשוב] יקבע, תחת הנחיית המנכ"ל ובתיאום עם אגף החירום במשרד, במידה וקיים, את יעדי ההתאוששות שלו במצב החירום, לרבות רמת התאוששות, וזמני התאוששות צפויים, עד לחזרה לתפקוד מלא בעת החזרה לשיגרה".

על פי נוהל מפתח<sup>10</sup>, תוכנית התאוששות מאסון כוללת תוכנית להתאוששות המערך הטכנולוגי. התוכנית כוללת את תהליך הפעלת מצב החירום, את תהליך החזרה ממצב החירום, את תרגילי החירום ומדדים עיקריים להתאוששות:

Return Point Objective (RPO) - כמות המידע שאבד (במונחי זמן פעילות) בהתרחש אסון.

Return Time Objective (RTO) - פרק הזמן המרבי מרגע קבלת ההחלטה עד להפעלת אתר החירום.

עם הקמתו החל האגף לעדכן את פק"ל שע"ם, שנכתב בשנת 2014. המסמך כולל רכיבים של תהליך הכנתה של תוכנית ההמשכיות העסקית והשפעתם על תשומות שע"ם ויחידותיו.

בשנת 2018 הסתיים עדכון הפק"ל בסיוע יועץ חיצוני נוסף מטעם רשות המיסים, אך לא צוינו בו היבטים מסוימים.

ביולי 2019 העביר הממונה על החירום ברשות המיסים לאגף המשכיות עסקית מסמך ובו הגדיר מספר יעדים.

הביקורת העלתה פערים בנוגע להשלמת תוכנית התאוששות מאסון. עוד נמצאו פערים בתהליך גיבוש תוכנית ההמשכיות העסקית ובהשלמתה. על שע"ם לתקן את הליקויים שעלו בתהליך גיבוש תוכנית המשכיות עסקית ובהשלמתה.

רשות המיסים מסרה בתשובתה כי תשלם את תיקון הליקויים בכפוף למשאבים הנדרשים.

מערך הדיגיטל הלאומי מסר בתשובתו מ-8.6.2022 כי עמדתו כעמדת משרד מבקר המדינה בנוגע להמשכיות עסקית ולהתאוששות מאסון.

## השפעותיו של היעדר תוכנית להמשכיות עסקית

היעדר תוכנית להמשכיות עסקית בשע"ם מצמצם את יכולתו של הארגון לתפקד במצבי חירום מסוימים, ואכן הדבר בא לידי ביטוי בעת משבר הקורונה. בתחקיר הפקת לקחים שנערך בשע"ם עלה כי לא הייתה לשע"ם תוכנית סדורה לפעולה בעת התפרצות המגפה, והמשבר נוהל אד הוק על ידי מנהלת שע"ם דאז בשיתוף צוות החירום. עוד עלה כי "מחסור במחשבים ניידים,

10 נוהל מפתח - קובץ נהלים גנריים שאימצה רשות התקשוב כבירית מחדל בהיעדר נוהל אחר שאישר המשדר.



והפגיעה במרכיבי שכר משמעותיים בעבודה מהבית (כמו כונוניות ושעות נוספות), גרמו לעובדים רבים להגיע למשרד, במגבלות התו הסגול, אך תוך תוספת סיכון לבריאותם ולבריאות שאר העובדים והגברת הסיכון לפגיעה בשירותים לרשות המיסים".

ממצאי התחקיר בדבר היעדר תוכנית להמשכיות עסקית בעת התפרצות מגפת הקורונה ממחישים את הצורך בהשלמת כתיבתה של התוכנית להמשכיות עסקית על פי הנחיות רשות התקשוב.

## ועדת היגוי להמשכיות עסקית

בשנת 2019 הוקמה בשע"ם ועדת היגוי להמשכיות עסקית. בראשות הוועדה עמדה מנהלת שע"ם דאז, והשתתפו בה נציגים משע"ם: הסמנכ"ל למינהל ומשאבי אנוש, מנהל אגף המשכיות עסקית ועובד מהאגף, מנהל אגף תשתיות ותקשורת, סמנכ"ל לית טכנולוגיות ומנהלת שירות לקוחות. בישיבתה הראשונה שהתקיימה באוגוסט 2019 צוין שהוועדה התכנסה כדי להניע מהלך של פיתוח תוכנית המשכיות עסקית בשע"ם. בישיבת הוועדה שהתקיימה ב-8.12.20 נקבע כי היא תתכנס אחת לרבעון.

בביקורת עלה כי לא הונפק כתב מינוי לחברי ועדת ההיגוי להמשכיות עסקית ולא נקבעו סמכויותיה. נוסף על כך, עד למועד סיום הביקורת התכנסה הוועדה פעם אחת נוספת, ביולי 2021, ולמעשה התכנסה שלוש פעמים עד למועד סיום הביקורת, ולא בכל רבעון כפי שנקבע בישיבתה.

מומלץ לוועדת ההיגוי להמשכיות עסקית להתכנס בהתאם לתדירות שנקבעה ולבחון את החסמים העומדים בפני קידום הפרויקט ואת הדרכים להסרתם.

## תרגול ובקרה שוטפים

כדי לשמור על כשירות המערכות ועל מקצועיותו של כוח האדם, יש לבצע תרגילים תקופתיים של המעבר לאתר ה-DR ושל תפעולו. במסמך מדיניות אבטחת מידע וסייבר של שע"ם נקבע כי שע"ם יבצע תרגול תקופתי בתדירות שתקבע הנהלת שע"ם, וזאת לשם בחינת אופן ההתאוששות ממצבי אסון.

בביקורת נמצא כי שלא בהתאם למסמך מדיניות אבטחת מידע וסייבר של שע"ם, הנהלת שע"ם לא קבעה את תדירות התרגול התקופתי הנדרש. עוד נמצא כי לשע"ם יש נוהל העוסק בתרגול המעבר לאתר ה-DR. הנוהל עוסק בהיבטים שונים הנדרשים לתרגול, אך לא נקבעה בנוהל תדירות התרגול.

בביקורת עלה כי תרגיל מסוים בוצע באופן חלקי.

מומלץ לשע"ם לשקול לבצע את התרגילים במתכונת מלאה, לקבוע בנוהל את תדירות התרגול והוראות מסוימות לתיקון הליקויים שנמצאו בתרגול.



## סיכום

שע"ם הוא גוף ה-IT של רשות המיסים, וכזוה הוא מפתח מערכות מידע עבודה, מתחזק מערכות קיימות ומחזיק במידע. על כן, יש חשיבות גדולה לרמה גבוהה של הגנת סייבר בשע"ם וכן לתפקוד מלא של שע"ם בעיתות משבר ולהתאוששות מהירה שלו מאסון.

ממצאי הביקורת מעלים כי על שע"ם לפעול לשיפור הגנת הסייבר על מערכותיו.

מומלץ כי שע"ם יפעל בהקדם לתיקון הליקויים שהועלו בדוח זה תוך בחינת יישום המלצות הדוח.