משרד הכלכלה והתעשייה
המנהל הכללי

מדיניות אבטחת מידע 5.2

גרסה – 1.2

תאריך יישום – **10 מאי , 2021**

ניהול שינויים

תאריך	מחבר	גרסה	ניהול שינויים
01.03.2019	ליאת אדלשטיין	1.0	מקור
19.1.2021	אבנר וקסמן	1.1	עדכון שוטף של שינויים
10.5.21	אבנר וקסמן	1.2	עדכון קוורום מינימום לוועדת סייבר
01.01.2022	להב יצחקי	1.2	אישור מחדש לשנת העבודה 2022

כללי

מסמכי עזר

כותרת	שם הקובץ
כלל נהלי אבטחת המידע	נהלי מנא"ם
מדיניות ארגונית	מדריך אבטחת מידע 4.0

הגדרות

1. בעלי העניין במשרד הכלכלה והתעשייה - יחיד או קבוצה או שותפים שיש להם זיקה מוקנית לארגון. בעלי העניין הם לא רק גורמי הנהלה אלא גם עובדי המשרד בארץ ובחו"ל, עובדי מיקור חוץ, ספקים, נותני שירותים, יועצים, תעשיינים ובעלי עסקים וכל הסביבה הארגונית והקהילתית במסגרתה פועל המשרד.
2. מנא"ם – המנא"ם היא מערכת ניהול אבטחת המידע אשר מדיניות זו, כמו גם מדריך אבטחת המידע ("המדריך") ומסמכים קשורים ותומכים נוספים מהווים חלק ממנה. המנא"ם תוכננה על בסיס הנחיות תקן ISO 27001:2013.
3. ISO 27001:2013 – תקן אבטחת מידע בינלאומי, שתפקידו לעצב מערכת אחידה לניהול אבטחת מידע בארגונים וכך גם במשרד הכלכלה והתעשייה. גרסת 2013 היא הגרסה העדכנית.
4. תקנות חוק הגנת הפרטיות - החוק המרכזי המסדיר את סוגיית הזכות לפרטיות בישראל. החוק מקיף את כל תחומי הגנת הפרטיות, נוגע לתחומי משפט שונים ומגדיר מהי פגיעה בפרטיות ובאילו מצבים היא מוצדקת. תקנות חוק הגנת הפרטיות מפרטות את אופן יישומה של חובת אבטחת המידע המוטלת בחוק הגנת הפרטיות הישראלי על כל גורם המנהל או מעבד מאגר של מידע אישי, בעת קביעת מנגנונים ארגוניים ודרישות מהותיות (ניטרליות טכנולוגית), שמטרתם הפיכת אבטחת המידע לחלק משגרת ניהול הארגון.

אחריות

1. בעלי העניין במשרד הכלכלה והתעשייה- להנהלה, לכלל העובדים בתצורות ההעסקה השונות (אזרחי ישראל, הנהלת משרד הכלכלה והתעשייה, מועמדים לעבודה, גורם מסמיך לתקן אבטחת מידע, עובדי

מדינה/מיקור חוץ/ספקים, המשק הישראלי) במשרה מלאה ובמשרה חלקית, לקבלני משנה, ליועצים לפרויקטים ולכל גורם חיצוני תהיה מודעות בנוגע לאחריותם לשמור על כללי אבטחת המידע, לדווח על כשלי אבטחה ולפעול בהתאם לדרישות המנא"ם. השלכות הפרת מדיניות האבטחה מתוארות בתקנון המשמעתי של משרד הכלכלה והתעשייה.

2. הנהלת משרד הכלכלה והתעשייה- להנהלת משרד הכלכלה והתעשייה (מנכ"ל משרד הכלכלה והתעשייה באמצעות מנב"ט המשרד) האחריות להגדרת צורכי המשרד בנושא אבטחת מידע, להקצאת המשאבים ולהעלאת המודעות בקרב העובדים. ראשי מינהלים / אגפים ומחלקות יישאו באחריות ישירה ליישום נהלי אבטחת המידע בתחומי סמכותם, לפעילות הולמת של עובדי המחלקה בהיבטי אבטחת המידע וכן לטיפול באירועי אבטחת מידע בשיתוף עם הגורמים הרלוונטיים במשרד.

3. וועדת היגוי לאבטחת מידע במשרד הכלכלה והתעשייה- וועדה ייעודית למנהל הגנת הסייבר לניהול אבטחת המידע. הוועדה תכונה "וועדת היגוי לאבטחת מידע". הצוות יורכב מנציגי אגפים במשרד הכלכלה והתעשייה אשר לתפקידיהם ולפונקציות שהם ממלאים קיימת נגיעה לנושא אבטחת מידע. תפקידי הועדה הוא אישור מדיניות אבטחת המידע, ביצוע הערכת סיכונים, מיפוי הסיכונים, ווידוא, יישום וביצוע של בקרות למזעור סיכונים פוטנציאלים.

4. מנהל הגנת הסייבר במשרד הכלכלה והתעשייה- מנהל הגנת הסייבר הוא הגורם הבכיר והמקצועי ביותר בתחום אבטחת המידע בארגון (משמש כיועץ למנהלי הארגון בתחום אבטחת המידע בארגון). באחריותו של מנהל הגנת הסייבר במשרד הכלכלה והתעשייה לוודא שמסמך זה על נהליו השונים מיושם ומבוקר בהתאם לדרישות שגובשו וסוכמו במנא"ם.

5. מנחה הגנת הסייבר במשרד הכלכלה והתעשייה - מנחה מקצועי בהובלת תחום אבטחת המידע בארגון המנחיל ויוזם דרכים למימוש החלטות ההנהלה בנושא. אחראי להקמת תשתית אבטחת המידע בארגון ולקיומם של סטנדרטים, נהלים והנחיות טכניות אשר יתמכו בתהליך זה. יוזם פעילות שוטפת של ניטור ובדיקה על מנת לוודא את אבטחתם של מערכות המחשוב במשרד.

6. בעלי המידע במשרד הכלכלה והתעשייה- בהתאם למנא"ם, האחריות האישית של כל בעל מידע בארגון תוביל את משרד הכלכלה והתעשייה ליצירת מודעות לתחום אבטחת המידע כאשר המטרה המרכזית הינה מניעה של גורם או פרט שאינו מורשה לגשת למידע או מערכת בעל ערך שיכול לפגוע בזמינותו, שלמותו ואמינותו של המידע המצוי בידי החברה.

7. בעל נכס (נכס: רכוש בין אם הוא פיזי או קנייני)- אחריותו של בעל הנכס היא קביעת רמת הסיווג של הנכס שבאחריותו תוך התאמת רמת הסיווג הקיימת לדרישות החוק. בנוסף, אחריותו לשלמות, זמינות ואמינות לשם כך עליו לוודא הימצאות בקרות מתאימות לנכסים באחריותו בהתאם לרמת סיווגם. על בעל הנכס האחריות לסיוע בהגדרת דרישות גיבוי ושחזור נתוני הנכס.

8. צוות המחשוב במשרד הכלכלה והתעשייה- אחראים להבטיח כי תשתית מערכות המידע במשרד הכלכלה והתעשייה תואם את דרישות מדיניות אבטחת המידע כפי שפורטו במנא"ם.
9. מנהל הביטחון במשרד הכלכלה והתעשייה- משמש באופן כללי כאחראי תחום האבטחה במשרד הכלכלה והתעשייה לכן נדרש ממנו לפקח ולבקר על כל בעל עניין אשר לו גישה לאזורים רגישים במשרד (ראה פרק אבטחה פיסית וסביבתית במנא"ם). בנוסף, עליו לספק לעובדי המשרד או לבעלי עניין אחרים פרטים על האזורים המאובטחים ועל הפעולות הנעשות בכדי למנוע גישה פיסית של גורמים לא מורשים, נזק או הפרעה למידע או לתהליכים בארגון.
10. כלל עובדי הארגון- להנהלה, לכל העובדים במשרה מלאה ובמשרה חלקית, לקבלני משנה, ליועצים לפרויקטים ולכל גורם חיצוני תהיה מודעות בנוגע לאחריותו לשמור על אבטחת מידע, לדווח על כשלי אבטחה ולפעול בהתאם לדרישות של המנא"ם. ההשלכות של הפרת מדיניות האבטחה מתוארות בתקנון המשמעתי של משרד הכלכלה והתעשייה.

היקף ותכולת המנא"ם (ISMS)

היקף ותכולת המנא"ם במשרד הכלכלה והתעשייה מכסה כמכלול וכיחידה שלמה את משרדי הנהלת משרד הכלכלה והתעשייה (כולל אזורים רגישים), המערכות, היישומים והתהליכים הפיזיים הרלוונטיים לתחום אבטחת המידע במשרד.

הגדרות ומטרות של המנא"ם (ISMS)

מערכת ניהול אבטחת המידע מוגדרת כחלק בלתי נפרד ממערכת הניהול הכוללת של הארגון בתחום אבטחת המידע. המנא"ם מגדיר באופן ברור ומפורט את מדיניות אבטחת המידע הארגונית, את הנהלים, התהליכים והמשאבים שהנהלת משרד הכלכלה והתעשייה אישרה בתחום אבטחת המידע. המנא"ם משמש ככלי ניהולי המאפשר למנהלי המשרד ולגורמי אבטחת המידע המקצועיים בו ליישם, לפעול, לבקר ולהטמיע את תהליכי העבודה הרלוונטיים לתחום אבטחת המידע.
המטרה המרכזית הינה יצירת מערכת אחידה לניהול מערך אבטחת המידע תוך שיפור הנהלים והתהליכים הארגוניים ומיפוי גורמי סיכון אפשריים לתקלות ואירועי אבטחת מידע.

מקור הדרישה לתקן

1. שמירה על המידע האגור במערכות המשרד כחלק אינטגרלי ממטרותיו.

2. שמירת האינטרסים של בעלי העניין במידע כמפורט במנא"ם ובטבלת בעלי עניין.
3. "יישור קו" אל מול סטנדרטים בינלאומיים בנושא אבטחת המידע.
4. אינטגרציה עם לקוחות, ספקים וארגונים מכל העולם.
5. התווית דרך סדורה לניהול מערך אבטחת המידע וצמצום הסיכון לדלף מידע.
6. התווית דרך סדורה לניהול וטיפול המידע במשרד.

תחום היישום

תחום היישום הפיזי הינו המבנה הראשי של משרד הכלכלה והתעשייה, בו נמצאים עובדיו, בו מעובד מידע רלוונטי לפעילות המשרד כולל:

1. משרד הכלכלה והתעשייה הינו ברחוב בנק ישראל 5 בירושלים, קיימים משרדים נוספים ברחוב אילת ודרך בגין בתל אביב וברח' הרטום 10 בירושלים.
2. ציוד מחשוב משולב מערכות מידע,
3. התחום הפיזי כולל גורמים נוספים (צד ג') העושה שימוש במידע וחצרותיהם. רשימת הספקים וגורמי החוץ נמצאים בקובץ ריכוז מידע המצורף לנהלי אבטחת המידע,
4. נכסים פיזיים ונכסי מידע – רשימת הנכסים נמצאת בקובץ ריכוז מידע המצורף לנהלי אבטחת המידע,
5. תהליכים עסקיים ורגישים במשרד המתקיימים בכלל מחלקותיו וע"י כלל עובדיו של המשרד. מיפוי וניתוח התהליכים נמצא בקובץ תהליכים המצורף לנהלי אבטחת המידע,
6. כלל המידע האגור במשרד במצעים לוגיים ופיזיים ועל כל נכס מידע אחר,
7. מדיניות זו תחול על כל עובדי הארגון. בהקשר זה עובדי הארגון הינם:
   7.1. הנהלה
   7.2. עובדי המדינה במשרה מלאה ובמשרה חלקית בארץ ובחו"ל.
   7.3. נותני שירותים - קבלני משנה / ספקים / יועצים - לכל גורם חיצוני תהיה מודעות בנוגע לאחריותו לשמור על אבטחת מידע, לדווח על כשלי אבטחה ולפעול בהתאם לדרישות המנא"ם.
   7.4. תעשיינים ובעלי עסקים.
   7.5. עובדי מיקור חוץ בדגש על עובדי ניקיון ומאבטחים.

7.6. מועמדים לעבודה במשרד הכלכלה והתעשייה.

8. כלל הציוד והאמצעים הטכנולוגיים הנמצאים בשימוש. רשימת הציוד והאמצעים מצורפים בקובץ ריכוז מידע המצורף לנהלי אבטחת המידע.

9. כלל התוכנות, המערכות והפלטפורמות העוסקות בנתונים, בין אם הן מותקנות בארגון והן במסגרת שירותי תוכנה מצד ג', כמפורט בסעיף 1.4 "נכסי מידע מרכזיים".

10. ועדת ההיגוי של הארגון מייצגת את הנהלת משרד הכלכלה והתעשייה (מנכ"ל המשרד) והיא המאשרת שינוי ו/או חריגה מתחום ומדיניות המנא"ם.

11. שותפי צד שלישי המחויבים לארגון.

12. קבלני משנה.

<u>פעילות במסגרת תחום היישום:</u>

1. מיפוי התהליכים הרגישים והעסקיים בתחומי יישום המנא"ם.

2. מיפוי נכסי המידע בתחומי יישום המנא"ם.

3. זיהוי וניהול סיכונים בתחומי יישום המנא"ם.

4. העלאת מודעות הגורמים הקשורים בתחום יישום המנא"ם.

5. אימון ותרגול הגורמים הקשורים בתחום המנא"מ.

6. ביצוע בקרות אבטחת מידע מול גורמים פנימיים וחיצוניים (ספקי צד ג').

7. בחינת הגבולות והתחומים מדי תקופה קצובה לצורך התאמה למצב קיים.

מטרות ויעדים ומדדים

מטרת הנוהל

קביעת מדיניות ברורה ומפורטת בנושא אבטחת המידע במשרד הכלכלה והתעשייה. מדיניות זו תחול על כל אדם המשתמש בנכסי המידע של משרד הכלכלה והתעשייה לרבות ספקים ומשתמשים חיצוניים. בהתאם להגדרות ולנהלים שגובשו ע"י המשרד, ונקבעו במנא"ם אשר אושרו ע"י ועדת ההיגוי בה נציגי הנהלת משרד הכלכלה והתעשייה. מדיניות זו תפורט במסמך זה ותהווה נוהל משלים לנהלי אבטחת המידע.

מטרת המדיניות

הגדרת מחויבות ההנהלה וכלל עובדי המשרד לעמידה בדרישות תקן ISO27001 ודאגה לשיפורו השוטף של המנא"ם.

**הערה- בכל מקרה של סתירה ו/או דו משמעות ו/או אי התאמה בין הוראותיה של מדיניות זו ו/או נספח מנספחי נהלי אבטחת מידע לבין הוראות ע"פ דין כלשהו, יגבר האמור בהוראות ע"פ דין, אלא אם כן נאמר במפורש אחרת. ובהקשר זה הוראות ע"פ דין הינן:

1. חוק הגנת הפרטיות.
2. סקר סייבר ע"פ מדד יה"ב.
3. ביקורות של מבקר הפנים של המשרד.
4. יצוין כי מדיניות אינה מהווה תחליף לנוהל "ניהול סיכוני סייבר".
5. נהלים ומדיניות שפורסמו ע"י המחוקק הנוגעים למשרדים ממשלתיים.

מטרות אבטחת מידע של הארגון

6. מטרות משרד הכלכלה והתעשייה, כארגון המעודד את הצמיחה הכלכלית של ישראל, הינן:

6.1. שמירת המידע אודות המשרד: רגישים, חסויים, שמורים או סודיים, בעלי רמת רגישות קריטית.

6.2. שמירת נכסי מידע ומערכות מידע קריטיות המשמשות את המשרד.

6.3. שמירה על זמינות אמינות ונגישות למידע.

6.4. מתן יכולת התאוששות מהירה במקרה של אירוע סייבר- קיים נוהל משלים בקיט הנהלים "תגובה לאירועי אבטחת מידע וסייבר".

יעדים ומדדים

1. <u>יעד על</u>

1.1 יישום וביצוע של 80% לפחות מתכנית העבודה לתחום אבטחת המידע אשר אושרה ע"י הנהלת המשרד בדגש על תהליכים טכנולוגיים וניהוליים, אשר נבחנו והוגדרו כברי סיכון ופגיעה בשלמות, זמינות ואמינות המידע של המשרד.

2. <u>יעדי ההנהלה לאבטחת מידע– (מנכ"ל המשרד) :</u>

2.1. עמידה במבדקי מכון התקנים הישראלי.

2.2. הקצאת המשאבים הנדרשים לתפעול ושיפור המנא"ם.

2.3. בקרה על מנהל הגנת הסייבר בארגון תוך וידוא קידום תהליכים וקבלת סטאטוס שוטף על עבודתו בתחומי התקן והמנא"ם.

2.4. הכרת תהליכי זרימת המידע בארגון ואבטחת מידע באופן ראוי.

2.5. התעדכנות שוטפת בתוצאות מבדקי מנא"ם שונים ביעילות המנא"ם ותפקוד ויעילות מערכות המידע במשרד.

2.6. יצירת סביבת עבודה מאובטחת ברמה התהליכית וברמה הטכנולוגית.

3. <u>מדדים אופרטיביים למעקב ובקרה ואמת מידה לאימות הישגים (שנתי):</u>

3.1. כינוס שתי ועדות היגוי לאבטחת מידע במהלך שנת עבודה.

3.2. תכנית עבודה רב שנתית על פני 3 שנים לסקירת מערכות המידע הארגוניות בהיבטי אבטחת מידע. סקירת כל מערכות הארגון בתוך 3 שנים.

3.3. שמירה על מבדקי הפיקוח של מכון התקנים שיבוצעו בשנה"ע ועמידה בישימות של 80% מתכנית העבודה.

3.4. סקירת 10 תהליכים לפחות במחלקות קריטיות במהלך שנת העבודה, כולל הפעלת הגנות א"מ לטיפול בממצאים שיתגלו.

3.5. מיפוי מאגרי המידע ברשות המשרד ורישומם במשרד המשפטים.

3.6. ביצוע 3 סקרי בקרת גישה בשנת העבודה על מערכות קריטיות. המערכות יקבעו בהתאם לרמת חשיבותן לארגון ובהתאם לסבירות להתממשות כשל במערכת.

3.7. יישום מלא של דרישות אבטחת מידע בתהליכי רכש.

3.8. מודעות עובדים- באחריות הנהלת המשרד למנות בעל תפקיד שמתוקף תפקידו יהיה לפעול למען שיפור מודעות העובדים לנושאי אבטחת מידע והגנת הסייבר:

3.8.1. ביצוע הדרכת מודעות אחת לשנה לכלל עובדי המשרד, ניתן ליישם באופן פרונטלי או באמצעות לומדה אלקטרונית אשר הצלחתה תוגדר כמדד חובה לכלל העובדים.

3.8.2. ביצוע הדרכה לעובדים חדשים טרם כניסה לתפקיד.

3.8.3. החתמת כל עובד על הצהרת סודיות עם קליטתו בארגון.

4. יעדים ומשימות ועדת ההיגוי למעקב ובקרה ואמת מידה לאימות הישגים:

4.1. הוועדה תעקוב אחר מבדקי מנא"ם פנימיים וסטאטוס תיקון ליקויים.

4.2. הוועדה תעקוב אחר סקרי סיכונים ומבדקי חדירה על המערכות השונות.

4.3. הוועדה תוודא את אפקטיביות ההדרכות המתבצעות אחת לתקופה לעובדי הארגון.

4.4. הוועדה תוודא את קיום מבדקי IQC (להלן הגורם המסמיך) אחת לתקופה אשר הוגדרה/ תוגדר ע"י הסוקר.

4.5. הוועדה תשתף פעולה עם מנהל הגנת הסייבר ותקיים סטאטוס תקופתי על ניטור ובקרה על המערכות השונות בארגון.

4.6. לאחר מיפויי כלל תהליכי זרימת המידע, הוועדה תשתף פעולה עם מנהל הגנת הסייבר ותבצע תהליכי ניטור ובקרה אשר יכללו את כלל תהליכי זרימת המידע במחלקות ארגון.

4.7. הוועדה תוודא ותעקוב אחר תוצאות המבחנים לאחר הדרכות של עובדי הארגון (בדיקת אפקטיביות).

4.8. הוועדה תבצע סקרי הנהלה אחת לתקופה בהתאם לנוהל .

4.9. בנוסף, גובשו מדדים לבדיקת אפקטיביות הכוללים יעדים להשגת מטרות באופן מספרי. אלו יקבעו ע"י ועדת ההיגוי. רשימת היעדים מופיעה בטבלת מדדים ובדיקת אפקטיביות.

הצהרת מנכ"ל המשרד

מנכ"ל המשרד אישר מדיניות אבטחת מידע עבור משרד הכלכלה והתעשייה. מדיניות זו מתוארת בהמשך והיא אושרה להפצה על ידי מנכ"ל משרד הכלכלה והתעשייה. הגרסה הנוכחית של המסמך, הנמצאת במשרדו של מנהל הגנת הסייבר, זמינה עבור כל צוות העובדים, כמו גם עבור קבלנים וגורמים חיצוניים.
מדיניות אבטחת המידע פותחה בתהליך של PDCA (תכנן-בצע-בדוק-פעל), כפי שהוא מתואר מטה:

1. תכנן (PLAN): כתיבת המנא"ם ואישורה ע"י מנכ"ל משרד הכלכלה והתעשייה- קביעת המדיניות, המטרות, התהליכים ונהלים רלוונטיים בהתאם למיפוי התהליכים הארגוניים בתחום אבטחת המידע במטרה ליישמה בכל המשרד. בשלב זה יקבעו יעדי המנא"ם במטרה לשמור על המידע הפרטי הרגיש של בעלי המידע . בנוסף, בשלב זה ייקבע כיוון כללי למטרות הארגון ולעקרונותיו בנושא אבטחת המידע: מחויבות לשמור על חשאיות, שלמות וזמינות של כלל הנכסים הפיסיים והאלקטרונים של משרד הכלכלה והתעשייה.

2. בצע (DO): הפעלת המנא"ם בפועל כחלק בלתי נפרד מתהליכי העבודה במשרד הכלכלה והתעשייה, הכוללים פעולות הטמעה ויישום אמצעי אבטחה, במטרה לעמוד ביעדים שהוגדרו עבור אמצעי אבטחה.
3. בדוק (CHECK): עריכת בקרה שוטפת על תפקוד המנא"ם ע"י פעולות ניטור ובחינה- זיהוי אירועי אבטחה (מוצלחים וכושלים כאחד), כדי לאפשר למנהלים הרלוונטיים להעריך את יעילות ומידת אכיפת נהלי האבטחה ולאפשר להם לנקוט בפעולות הנדרשות על מנת למגר פרצות אבטחה, לאור סדרי העדיפויות של המשרד.
4. פעל (ACT): הפקת לקחים והטמעתם הכוללים תחזוקה ושיפור- גיבוש נהלים כתובים בנוגע לפעולות מתקנות ומונעות הקשורות למנא"ם.

מחויבות ומעורבות ההנהלה לתקן ולאבטחת מידע

1. הנהלת משרד הכלכלה והתעשייה אחראית לוודא קיומם של עקרונות אבטחת מידע נאותים ולשמור עליהם על מנת להגן על נכסי המידע של המשרד ושל בעלי המידע, מפני דליפה, שינוי או מחיקה.
2. הנהלת משרד הכלכלה והתעשייה משמשת בעיקר בתור גורם-על בעל סמכות בתחום אבטחת המידע, דוגמת יישום מדיניות ההנהלה, כתיבת תכנית עבודה, השתתפות בדיונים תקופתיים, קביעת סקרי אבטחת מידע בתדירות קבועה ודיון בממצאים חריגים שעלו בסקרים אלה.
3. מנהלי המשרד, שהוגדרו כחברי וועדת ההיגוי לאבטחת מידע, יבצעו ביקורות שוטפות וביקורות פתע על פעילות מחלקות הארגון ו/או נכסי הארגון כדי להבטיח כי פעילות המשרד מבוצעת בהתאם לנהלי אבטחת מידע שקבע המשרד במנא"ם.
4. הנהלת משרד הכלכלה והתעשייה תתכנס פעמיים בשנה לצורך סקר אבטחת מידע, המוגדר כ"וועדת היגוי לאבטחת מידע וסיכוני סייבר". מטרת הכינוס היא מעקב ומדידה של יישום צעדים בתחום אבטחת המידע במשרד, והצבת משימות ומטרות לשיפור בהמשך. כמו כן, אחת לשנה תבוצע סקירה של מסמכי המדיניות והנהלים ע"י גורמי המקצוע לצורך בדיקת רלוונטיות וישימות בהתאם לדרישות אבטחת המידע שהוגדרו. בתום תהליך סקירת הנהלים, יועלו העדכונים בפני וועדת ההיגוי לצורך קבלת אישור.

הועדה תורכב מבעלי התפקידים הבאים:

1. מנכ"ל (באפשרותו לקבוע בא כוחו)
2. מנב"ט המשרד הממונה הגנת הסייבר במשרד הכלכלה והתעשייה.

3. אחראי תחום אבטחת מידע.
4. מנהל אגף בכיר טכנולוגיות דיגיטליות ומידע.
5. מנהל אבטחת מידע.
6. סמנכ"ל בכיר למינהל ומשאבי אנוש.
7. מנהל אגף תקציבים.
8. חשב המשרד.
9. יועצת משפטית.
10. יועץ מטעם החברה המלווה לתקן ISO27001.
11. נציג יה"ב.

זימון וועדת היגוי

1. בשגרה, מנכ"ל משרד הכלכלה והתעשייה יזמן אחת לחצי שנה את בעלי התפקידים בסעיף הקודם לצורך כינוס וועדת היגוי.
2. שלא בשגרה, יזמן מנכ"ל משרד הכלכלה והתעשייה את חברי וועדת ההיגוי בהתקיים התנאים הבאים:
   2.1. התרחש אירוע אבטחת מידע אשר תוצאותיו מחייבות כינוס הוועדה לקבלת החלטות-המשך.
   2.2. הטמעת מערכת מידע חדשה במשרד המוגדרת כמערכת קריטית בעבורו.
   2.3. שינוי תכנית העבודה המצריך קבלת אישור הנהלה, בהתאם לנוהל "ניהול שינויים".
   2.4. אישור תקציב למשימה / פרויקט / אירוע בתחום אבטחת המידע.
   2.5. קוורום מינימום לקבלת החלטות:
      2.5.1. מנכ"ל (בסמכותו למנות ממלא מקום)
      2.5.2. מנהל אגף בכיר טכנולוגיות דיגיטליות ומידע.
      2.5.3. נציגות של יועמ"ש המשרד.
      2.5.4. מנב"ט המשרד הממונה על הגנת הסייבר במשרד.

הועדה אחראית על ההיבטים הבאים:

1. קביעת יעדים ומדדים לביצוע בשנת העבודה הנוכחית תוך בקרה על יישום יעדי השנה הקודמת.

2. בקרה על המענה לדרישות ה"מסגרת לניהול הסיכונים" המאושרת, הקבוע בתכנית אבטחת המידע במשרד.
3. בקרה על קיום תהליך הערכת סיכונים לפי המתודולוגיה המוצגת במנא"ם.
4. ניסוח, בחינה ואישור שינויים או תיקונים למדיניות אבטחת המידע.
5. לוודא שהארגון זיהה מה הן הפעולות הנחוצות לצורך הטמעת מדיניות אבטחת המידע, שיש לו את המשאבים הנדרשים לצורך ביצוע הפעולות הללו ושהוא משלב עקרונות של אבטחת מידע בכל התהליכים הרלוונטיים.
6. לנהל ולהנחות את פעולות מנהל הגנת הסייבר, כך שיתבצעו באופן מתואם בכל רחבי הארגון.
7. לבחון את האפקטיביות של הטמעת מדיניות אבטחת המידע.
8. לספק כיוון ברור ותמיכה גלויה ביוזמות של אבטחת מידע, גם באמצעות דוגמה אישית.
9. לאשר חלוקת תפקידים וסמכויות ברחבי המשרד.
10. ליזום תכניות להעלאת מודעות לנושא אבטחת המידע.
11. לוודא הטמעת אמצעי אבטחת מידע ברחבי המשרד.

תוצרים:

1. בסיום כינוס וועדת ההיגוי יופץ דו"ח ע"י מנכ"ל משרד הכלכלה והתעשייה. אשר יכיל את הנושאים הבאים:
   1.1. תאריך קיום הוועדה.
   1.2. משתתפי הוועדה.
   1.3. סיבת כינוס הוועדה (שגרה או כינוס נוסף).
   1.4. עיקרי הנושאים שהוצגו בוועדה.
   1.5. החלטות ההנהלה- נושא, הפעולה הנדרשת, גורם אחריות, לו"ז.
   1.6. טבלת יעדים וממדים- סטאטוס תכנון מול ביצוע.
2. נציג ההנהלה יסקור את תוכן הדו"ח ויחתום כי מאשר את כלל הנושאים הרלוונטיים כמפורט בסעיף 1.

הגדרת אבטחת מידע

שיפור מתמיד – להנהלה, לכל העובדים במשרה מלאה ובמשרה חלקית, לקבלני משנה, ליועצים לפרויקטים ולכל גורם חיצוני תהיה מודעות בנוגע לאחריות שלו (אשר מוגדרת בתיאור התפקיד או בהסכם) לשמור על אבטחת מידע, לדווח על כשלי אבטחה ולפעול בהתאם לדרישות המנא"ם. ההשלכות של הפרת מדיניות האבטחה מתוארות בתקנון המשמעתי של משרד הכלכלה והתעשייה ונציבות שירות המדינה. צוות עובדי המשרד יקבל הכשרות כדי לעורר מודעות לאבטחת מידע. עובדים בעלי מומחיות ספציפית יזכו להכשרות שמותאמות במיוחד עבורם בנושא אבטחת מידע.

זמינות – המידע והנכסים הקשורים למידע יהיו זמינים לעובדים מורשים בכל עת ויאובטחו מבחינה פיסית ולוגית. רשת המחשבים תוגדר כך שיכולת ההתאוששות שלה תהיה מהירה ומשרד הכלכלה והתעשייה יזהה ויגיב במהירות לתקריות אשר מאיימות על זמינות המידע, הנכסים והמערכות. הארגון יחזיק תכנית המשכיות עסקית (כמפורט בנוהל "תהליך המשכיות עסקית").

סודיות – על משרד הכלכלה והתעשייה לוודא שהמידע נגיש רק למי שמורשה לגשת אליו ומכאן שהמטרה היא למנוע גישה של משתמשים שאינם מורשים למידע של משרד הכלכלה והתעשייה, לידע שנמצא בבעלות המשרד ולמערכות המשרד, כולל רשת/רשתות התקשורת, אתר/אתרי האינטרנט, הרשת החיצונית/הרשתות החיצוניות וכל המערכות הרלוונטיות של הארגון (בין אם הגישה נעשתה באופן מכוון ובין אם היא נעשתה באופן שאינו מכוון)- קיים נוהל משלים בקיט הנהלים בנושא "מדיניות בקרת גישה".

שלמות – רכיב זה כולל הגנה על שלמות, דיוק ושיטות העיבוד של המידע במשרד הכלכלה והתעשייה ומכאן שהוא דורש מהמשרד למנוע כל שינוי בנכסים פיסיים או במידע אלקטרוני, בין אם שבוצע בטעות או בכוונת זדון, באופן מלא או חלקי, ובין אם מדובר בשינוי לא מאושר או בהשמדה של נכס או של מידע. המשרד יחזיק בתכניות לגיבוי ולשחזור מידע, ידווח על תקריות אבטחה ויעמוד בדרישות החוק הרלוונטיות בנושא מידע.

הנכסים הפיסיים של משרד הכלכלה והתעשייה כוללים, אך אינם מוגבלים ל: רכיבי החומרה של המחשבים, כבלי תקשורת, מערכות טלפוניה, מערכות תיוק וקבצים פיסיים.

הנכסים והמידע הארגוני (Information Assets) כוללים כל מידע מודפס או כתוב על נייר, מועבר בדואר או מופיע בסרטים או כזה שנאמר בשיחה, כמו גם מידע שנשמר בצורה אלקטרונית בשרתים, אתר/אתרי אינטרנט, רשת/רשתות חיצוניות (extranet), מחשבים, מחשבים ניידים, טלפונים סלולריים, התקני אחסון חיצוניים, קלטות גיבוי וכל מידע דיגיטלי או מגנטי או מידע המועבר בצורה אלקטרונית, בכל דרך שהיא. המונח "מידע" כולל גם הנחיות שימוש במערכת המידע (מערכות הפעלה, אפליקציות, כלים וכדומה).

בהקשר זה- הנחיות האבטחה לנכסי מידע יבוצעו כדלהלן:

1. מידע מודפס- יישמר בארון, מגרה המצויים בחדר נעול של בעל התפקיד המוגדר כבעל המידע. יצוין כי מסדרונות המשרד אינם מוגדרים כאזור מאובטח.
2. מידע דיגיטלי - מידע השמור בשרתים, מחשבים, מחשבים ניידים, טלפונים סלולריים, התקני אחסון חיצוניים, קלטות גיבוי וכל מידע דיגיטלי או מגנטי או מידע המועבר בצורה אלקטרונית – יאובטחו ויגובו כמתחייב בהתאם למצוין בנוהל "סיווג מידע" באחריות מנהל הגנת הסייבר.

המנא"ם היא מערכת ניהול אבטחת המידע אשר מדיניות זו, כמו גם מדריך אבטחת המידע ("המדריך") ומסמכים קשורים ותומכים נוספים מהווים חלק ממנה. המנא"ם תוכננה על בסיס ההנחיות של תקן ISO 27001:2013.

כשל אבטחה הוא כל תקרית או פעולה אשר גורמים, או יכולים לגרום, לפגיעה בזמינות, בחשאיות או בשלמות הנכסים (information assets) הפיסיים או האלקטרונים של המשרד.

שינוי גרסאות (נהלים / הוראות עבודה / מסמכים)

1. פרק זה דן בעדכון של נהלים, הוראות עבודה ומסמכים מבוקרים כלליים בארגון.
2. פעולות אלו מאפשרות לקורא לדעת מהי הגרסה העדכנית ביותר, האם שונה לאחרונה, מה מהות השוני מהגרסה הקודמת ואת זהות הגורם המאשר את המסמך (כולל כל תיקונים שהוכנסו בו).

<u>עדכון נהלים:</u>

1. נוהל יעודכן אם:
   1.1. השתנו תנאי עבודה, שיטות עבודה או מבנה ארגוני.
   1.2. חל שינוי בחוק, בתקנה, בטכנולוגיה, בהנחיה או בשיטה לפיה עובדים במשרד ולשינוי השלכה על שיטת העבודה.
   1.3. הוצגו מסקנות והנחיות לעדכון נהלים בעקבות מבדק התאמה לתקנים (פנימי או חיצוני).
   1.4. הנוהל נסקר על ידי בעל תפקיד בארגון או במחלקה אשר קבע כי יש צורך בעדכון.
   1.5. לא יבוצע עדכון בנוהל ללא שיתופו של הגורם המאשר את הנוהל, או ממלא מקומו בתפקיד. גרסה מעודכנת של נוהל חייבת גם היא באישור של מנכ"ל משרד הכלכלה והתעשייה והמנהל המאשר. לא יאושרו שינויים במסמכים מבוקרים אלא על-ידי הגורם הממונה על הנהלים או האחראי על בקרת תיעוד.
   1.6. עדכון הנוהל יבוצע לפי השלבים המתוארים בסעיפים הבאים: המנהל האחראי יטיל על עובד להכין את טיוטת העדכון, עובד זה יוודא שהמסמך מאושר על ידי המנהל האחראי על כל הפעילויות עליהן

הוא חל ושמסמכים נוספים הקשורים למסמך הנדון, ושהעדכון שנעשה משפיע על הכתוב בהם, עודכנו ואושרו גם הם.

1.7. לפי שיקולו של המנהל האחראי על הפעילויות המתוארות בנוהל, תתוכנן הדרכה לעובדים על מהות השינויים בנוהל והתהליכים המעודכנים המתוארים בו. ההדרכה תתואם עם הממונה על הנהלים.

1.8. לקראת הפצת העדכון של מסמך, הממונה על הנהלים (או האחראי על בקרת התיעוד בארגון, יעדכן את שדות המהדורה ותאריך התוקף במסמך.

1.9. הממונה על הנהלים יפיץ את הנוהל המעודכן כמתואר בסעיף לעיל. הוא יודיע לכל העובדים על עדכונו של המסמך ויוודא שהדרכות נדרשות בנושא תוכננו ובוצעו לפני תאריך התוקף של העדכון.

1.10. ביום תחילת התוקף, באחריות כל עובד לסלק הדפסות, גרסאות נייר או העתקים אחרים של המסמכים הישנים בהם השתמש, ממקומות הימצאותם (אם ישנם). בפרט ישימו לב לסילוקם ולהחלפתם של עותקי מסמכים מבוקרים המוצגים על קירות, לוחות, מחשבים או ציוד כלשהו.

1.11. ללא קשר לאמור לעיל, כלל נהלי אבטחת המידע יובאו לאישור ועדת היגוי לאבטחת מידע בכל תחילת שנה קלנדרית.

מדיניות שולחן עבודה וצג נקי

הארגון אימץ מדיניות שולחן נקי מניירות ומהתקני אחסון נשלפים וגם מדיניות נעילת מסך עבור מערכות עיבוד מידע.

1. אין להשאיר מידע רגיש על שולחנות ללא השגחה (סיסמאות, מסמכים וכיוצ"ב).
2. יש לגרוס מידע רגיש באמצעות מגרסות פתיתים בתקן DIN 4 בלבד.
3. נעילת כל מסמכים וציוד אישי (מפתחות, תגים, חותמות) בארון/מגירה.
4. בעת עזיבת העמדה לזמן קצר ,יש ללחוץ על סימן נעילת המסך במחשב האישי או לחילופין ללחוץ על המקשים CTRL+ALT+DELETE בו זמנית ולבחור "לנעול את המחשב" ("LOCK COMPUTER").
5. בעת עזיבת העמדה לזמן ארוך או בסיום יום עבודתך, יש לבצע LOG OFF.
6. בהקשר זה- הנחיות האבטחה למידע המצוי במשרד / תחנת עבודה יבוצע כדלהלן:

6.1. מידע מודפס- יישמר בתוך ארון, מגרה שבחדר נעול של בעל התפקיד המוגדר כבעל המידע. (יצוין כי מסדרונות המשרד אינם מוגדרים כאזור מאובטח). מידע המוגדר כסודי יישמר בתוך ארון נעול בחדר נעול בסיום כל יום עבודה.

6.2. מידע דיגיטלי - מידע השמור בשרתים, מחשבים, מחשבים ניידים, טלפונים סלולריים, התקני אחסון חיצוניים, קלטות גיבוי וכל מידע דיגיטלי או מגנטי או מידע המועבר בצורה אלקטרונית – מנהל הגנת הסייבר ידאג להעביר הוראות אבטחה מעת לעת המציינות את הנחיות האבטחה הנדרשות.

7. שימוש בסיסמאות:

7.1. משתמשי המשרד יפעלו בהתאם למדיניות הסיסמאות ויבחרו סיסמה בהתאם לנוהל הסכם המשתמש עליו הם חתומים.

7.2. חל איסור מוחלט על מסירת סיסמאות למערכות עיבוד המידע של המשרד לגורמים שאינם מורשים, עברה זו נחשבת כעברת משמעת חמורה בעיניי המשרד. יובהר, הסיסמה הינה אישית ואינה ניתנת או מיועדת להעברה.

נהלי אבטחת מידע משלימים למדיניות זו

1. בהתאם להוראות תקן ISO27001 נכתבו נהלי אבטחת מידע משלימים למדיניות זו. נהלים אלה ייגזרו ממדיניות אבטחת המידע ומצרכי אבטחת המידע במשרד ומהווים הרחבה למצוין במדיניות זו.

2. ההנהלה תאשר את הנהלים עם כתיבתם או את השינויים המהותיים בהם ותפעל להטמעתם.

3. כמו כן, אחת לשנה תבוצע סקירה של מסמכי המדיניות והנהלים ע"י גורמי המקצוע לצורך בדיקת רלוונטיות וישימות בהתאם לדרישות אבטחת המידע שהוגדרו. בתום תהליך סקירת הנהלים, יועלו העדכונים בפני וועדת ההיגוי לצורך קבלת אישור.

4. רשימת הנהלים בהתאם למצוין בטבלה מטה:

מס"ד	שם הנוהל	מטרת הנוהל
1.	מדריך לניהול אבטחת מידע (מנא"מ) נוהל מספר 4.0	מערכת ניהול אבטחת המידע מוגדרת כחלק בלתי נפרד ממערכת הניהול הכוללת של המשרד בתחום אבטחת המידע. המנא"מ מגדיר באופן ברור ומופרט את מדיניות אבטחת המידע הארגונית, את הנהלים, התהליכים והמשאבים שהנהלת המשרד אישרה בתחום אבטחת המידע. המנא"מ משמש ככלי ניהולי המאפשר למנהלי המשרד ולגורמי אבטחת המידע המקצועיים במשרד ליישם, לפעול, לבקר ולהטמיע את תהליכי העבודה הרלוונטיים לתחום אבטחת המידע. המטרה המרכזית הינה יצירת מערכת אחידה לניהול מערך אבטחת המידע תוך שיפור הנהלים, התהליכים הארגוניים ומיפוי גורמי סיכון אפשריים לתקלות ואירועי אבטחת מידע. (מה נדרש)

		קבצים משלימים- תכנית עבודה, טבלת יעדים ומדדים, ביקורות מנא"מ פנימיות, הצהרת ישימות, סיכומי ועדות היגוי, טבלת בעלי עניין, טבלת מיפוי נכסי מידע, טבלת ספקים, מודעות עובדים והדרכות, כתבי מינוי, כלל נהלי אבטחת מידע.
.2	מדיניות אבטחת מידע נוהל מספר 5.2 + תקציר מדיניות אבטחת מידע לפרסום לעובדי המשרד	קביעת מדיניות ברורה ומפורטת בנושא אבטחת המידע במשרד הכלכלה והתעשייה. מדיניות זו תחול על כל אדם המשתמש בנכסי המידע של משרד הכלכלה והתעשייה בהתאם להגדרות ולנהלים שהמשרד גיבש וקבע במנא"מ. מטרת המדיניות הינה הגדרת מחויבות ההנהלה לעמידה בדרישות תקן ISO27001 ודאגה לשיפורו השוטף של המנא"מ. (איך נדרש). תקציר מדיניות אבטחת מידע הינה קובץ מתומצת של המדיניות הכללית זאת לשם פרסומה לכלל עובדי הארגון. קבצים משלימים- תכנית עבודה, טבלת יעדים ומדדים, טבלת מדיניות סיסמאות, מודעות עובדים והדרכות,
.3	הסכם משתמש נוהל מספר 6.1	קביעת מדיניות ברורה ומפורטת בנושא הסכם וניהול המשתמש במשרד הכלכלה והתעשייה. מדיניות זו תחול על כל אדם המשתמש בנכסי המידע של משרד הכלכלה והתעשייה ואשר במסגרתו הוא מאשר בצורה מפורשת (באמצעות חתימה על הסכם) את מדיניות אבטחת המידע של המשרד, בהתאם להגדרות ולנהלים שהמשרד גיבש וקבע במנא"מ כדוגמת: שימוש נאות במשאבי המשרד (מחשבים / דוא"ל / אינטרנט) קבצים משלימים- תקציר מדיניות אבטחת מידע.
.4	מסגרת לניהול סיכונים נוהל מספר 6.1.1 + נוהל הערכת סיכונים נוהל מספר 6.1.2	פירוט ומתודולוגיה לתהליך הערכת סיכונים שמטרתו לזהות ולהעריך סיכונים (כולל סיכונים הקשורים לאבטחת מידע) בתוכנית הארגונית, לזהות ולהעריך את האפשרויות השונות לצורך טיפול בסיכונים הללו ולבחור את אמצעי האבטחה אשר יפחיתו את הסיכונים הללו לרמה נסבלת, וזאת בהתאם לתוכנית הארגונית, לדרישות האופרטיביות, לאילוצים ולמטרות של המשרד, כמו גם לחוקים ולרגולציות פנים-מדינתיים ובינלאומיים בהתאם למצוין במנא"מ. הנהלים יפרטו את השיטה לביצוע הערכת הסיכונים. קבצים משלימים- טבלת ממצאים מביקורות, טבלת סיכוני אבטחת מידע, טבלת נכסים, טופס מדדי אבטחת מידע לבחינת מערכת חדשה, סקרי סיכונים טכנולוגיים.
.5	נוהל גורמים חיצוניים נוהל מספר 6.2	הארגון יגבש נהלים בנוגע לזיהוי סיכונים למידע, לנכסים ולמערכות עיבוד מידע אשר נובעים מתהליכים ארגוניים בהם מעורבים גורמים חיצונים. בנהלים יפורטו אמצעי האבטחה הנדרשים לפני מתן גישה למידע עבור גורמים חיצוניים במטרה לשמור על אבטחת מערכות עיבוד המידע במשרד, על הנכסים והמידע הארגוניים אליהם מתחברים או ניגשים גורמים חיצוניים ועל נכסים ומידע אשר מעובדים ומנוהלים על

		ידי גורמים חיצוניים. הסיכונים עבור גורמי צד שלישי יוערכו בהתאם לדרישות מכל ספק בנפרד או עפ"י חלוקה לתחומים עיסוק ולרמת הסיכון העולה מההתקשרות עם הספק. קבצים משלימים- טבלת ספקים, מדיניות בקרת גישה, דו"ח התחברות ספקים, מבדקי ספקים.
.6	נוהל סיווג מידע נוהל מספר 7.2	מתן כלים למשרד ע"מ לוודא שמוגדרת רמה מתאימה של הגנה על מידע. המידע במשרד הכלכלה והתעשייה יסווג על בסיס קריטריונים של ערך, דרישות משפטיות, רגישות ומידת הקריטיות של המידע עבור המשרד. קבצים משלימים- טבלת נכסים.
.7	נוהל אבטחת משאבי אנוש נוהל מספר 8.1	הגדרת הליך מוסדר, מובנה וידוע לקליטה, ניוד ועזיבה בהיבט אבטחת מידע. קביעת הליך מוגדר, כי העובד שנקלט עומד בדרישות, בכישורים ובמהימנות המוגדרים בתפקיד וכן בעת קליטה ועזיבה. הפחתת סיכונים הנובעים מטעויות אנוש, גניבה, הונאה או שימוש לרעה בנכסי מידע. קבצים משלימים- טבלת פרופילי תפקיד, סקרי בקרות גישה, דגשי אבטחת מידע לעובד חדש, הסכם משתמש.
.8	נוהל תכנון וקבלת מערכות נוהל מספר 10.10	קביעת מדדים ברורים במסגרת תהליך קבלה ואישור מערכות מידע לרבות, שדרוגים או גרסאות חדשות, המוצעים למשרד הכלכלה והתעשייה או הנדרשים על ידו בטרם כניסתן למשרד. תהליך זה מבקש להבטיח את התאמת המערכות למדיניות המשרד בתחום אבטחת המידע. כחלק מתהליך הפיתוח תבוצענה בדיקות התאמה למערכות (יעילות המערכת, עלות המערכת, הצורך במערכת וכד') בכדי להפחית סיכוי לכשלי מערכת. קבצים משלימים- טופס מדדי אבטחת מידע לבחינת מערכת חדשה.
.9	נוהל הגנה מפני קוד זדוני נוהל מספר 10.12	יישום אמצעי אבטחה שמאפשרים לזהות ולמנוע קוד זדוני ולהתאושש ממנו, כמו גם נהלים מתאימים לצורך עידוד מודעות של משתמשים לקוד זדוני. קבצים משלימים- טבלת מיפוי נכסי מידע.
.10	נוהל גיבוי מערכות נוהל מספר 10.13	מדיניות המשרד היא שהוא פועל במטרה לשמור על השלמות והזמינות של מידע ושל מערכות עיבוד מידע על ידי פיתוח מדדים ונהלים שגרתיים במטרה לוודא שכל הנכסים והמידע הארגוניים מגובים ושקיימים נהלים בדוקים המאפשרים שחזור שלהם בתוך מסגרת זמן סבירה. קבצים משלימים- טבלת מיפוי נכסי מידע.
.11	מדיניות בקרת גישה נוהל מספר 11.1	הגדרת העקרונות למתן זכויות גישה למערכות מידע ושירותי מידע. מטרת הנוהל להגדיר כי עבור כל משתמש וכל אובייקט במערכת ישנן הרשאות גישה מסוימות. כמו כן, הנוהל מפרט את המתודולוגיה לביצוע סקרי בקרות גישה על נכסי הארגון. קבצים משלימים- טבלת פרופילי תפקיד, סקרי בקרות גישה.

12.	נוהל ניהול שינויי אבטחת מידע נוהל מספר 14.2	מטרת נוהל זה היא גיבוש נהלים פורמליים של בקרת שינויים - כאשר מתבצע שינוי למערכות המשרד ו/או שינוי של תהליך הקשור לתחום אבטחת מידע במשרד יש לבחון, לבדוק ולהביא לאישור גורמי הנהלה על מנת לוודא שהשינוי אינו משפיע לרעה על פעולות המשרד או על אבטחת המשרד. קבצים משלימים- פורמט ניהול שינויים, טופס מדדי אבטחת מידע לבחינת מערכת חדשה.
13.	נוהל תגובה לאירועי אבטחת מידע וסייבר. נוהל מספר 16.1	מתן כלים למשרד ע"מ לוודא כי המענה לתקריות אבטחת מידע יהיה מהיר, אפקטיבי ומסודר, דבר המאפשר לוודא שהפעולות המתקנות או המונעות המתאימות יתבצעו, במטרה להחזיר את המערכת לתפקוד רגיל מהר ככל האפשר ולוודא שזוהו הזדמנויות לשיפור המערכת ושפעולות השיפור המתאימות מתבצעות. קובץ משלים פורמט דווח לאירועי אבטחת מידע.
14.	נוהל איסוף ראיות נוהל מספר 16.2	בכל תקריות אבטחת המידע, לא משנה אם הפעולה שננקטה בעקבות התקרית כללה פעולה משפטית כלשהי (אזרחית או פלילית) כנגד משתמש או משרד שמעורב בתקרית, יש לאסוף ראיות, לשמור אותן ולהציגן כפי שמפורט בהמשך, וזאת במטרה לאסוף ראיות בהתאם. בכלל מערכות המשרד תתקיים פונקציה של איסוף לוגים זאת ע"מ שבעת אירוע או חשש לאירוע ניתן יהיה לאסוף ראיות בהתאם. קובץ משלים פורמט דווח לאירועי אבטחת מידע.
15.	נוהל אבטחת מידע בהמשכיות עיסקית נוהל מספר 17.1.2	נוהל זה מפרט את התהליך הניהולי במטרה להבטיח המשכיות עסקית במשרד הכלכלה והתעשייה. התהליך מתייחס לדרישות אבטחת המידע שנחוצות על מנת להבטיח המשכיות עסקית של משרד הכלכלה והתעשייה במטרה לנטרל הפרעות לתפקוד המשרד, להגן על תהליכים ארגוניים קריטיים מההשלכות של כשלים משמעותיים במערכות המידע או אסונות ולוודא שהמערכות חוזרות לתפקד תוך פרק זמן הקצר ביותר.
16.	נוהל מאגרי מידע במשרד הכלכלה נוהל מספר 18.1	נוהל זה מפרט את התנהלות משרד הכלכלה בכל הטיפול במאגרי מידע ע"פ. חוק חופש המידע, תשנ"ח-1998.
17.	נוהל חופש המידע במשרד הכלכלה נוהל מספר 20.1	נוהל זה מפרט את התנהלות משרד הכלכלה בכל הטיפול במידע המועבר מהמשרד לגורמי חוץ ע"פ בקשות הנובעות מחוק חופש המידע.
18.	עדכוני טלאים באבטחת מידע נוהל מספר 23.1	נוהל זה מפרט את התהליכים ונהלים להתקנת טלאים PATCH לאבטחת מערכות המחשב של משרד הכלכלה והתעשייה.

19.	מדריך ניהול אבטחת מידע נוהל מספר 4.0	אבטחת מידע הינה כלל האמצעים הטכנולוגיים והארגונים הננקטים לשמירה על סודיות, שלמות וזמינות המידע. מדריך לניהול אבטחת מידע זה שנכתב ע"י TRIAD SECURITY מציג עקרונות מנחים ליישום אבטחת המידע ומייצג את תפיסת הנהלת המשרד בנושא זה:
20.	מצבי כוננות סייבר מספר נוהל 22.1	נוהל זה מפרט את קביעת סדר פעולות ברור, מוגדר ומפורט לפעילות משרד הכלכלה והתעשייה על כלל יחידותיו במצבי הכוננות המשתנים.
21.	נוהל חיבור מצלמות ודגשי אבטחת מידע לניהול שיחות ועידה בווידאו מספר נוהל 9.1ז	נוהל זה מפרט את מדיניות המשרד בצורה ברורה ומפורטת בנושא חיבור ושימוש במצלמות לצורך ביצוע שיחות ועידה בווידאו.
22.	אבטחת מכשירים ניידים מנוהלים מספר נוהל 23.1	הנוהל מפרט את תהליך אבטחת המכשיר הנייד המחובר של העובדים. בכדי צמצום האפשרות לכשל אבטחת מידע במידע הארגוני השמור במכשירים הניידים, וכן לצמצם הפגיעה בפרטיות עובדי משרד הכלכלה והתעשייה. הגדרת גורמי האחריות והסדרת אופן פעילותם של כלל הגורמים במשרד הכלכלה והתעשייה בכל הנוגע לניהול ואכיפת מדיניות אבטחת המידע למכשירים ניידים.
23.	נוהל חיבור מחשב לעבודה מרחוק נוהל מספר 8.1	הנוהל יפרט מדיניות ברורה בנושא עבודה מרחוק של עמ"זים ברחבי העולם ועובדי המשרד כאשר הם אינם יכולים להגיע למשרדים עקב מגבלות מחלת הקורונה בארצם. וחיבורים מרחוק של מחשבים לעבודה בטוחה.
24	שימוש במצעים ניידים	הנוהל יפרט הוראות לכלל עובדי הארגון ע"מ לוודא שמוגדרת רמה מתאימה של הגנה על המידע המצוי על גבי מצעים ניידים ואת אופן

	נוהל מספר 24.1	ניהול מצעים ניידים בהתאם לסיווג המידע המצוי בהם, על מנת למנוע חשיפה, גילוי או אובדן של מידע המצוי על גבי מצע נייד לגורם בלתי מורשה.

ממונה הגנת הסיבר הוא הבעלים של מסמך זה והוא אחראי לוודא שמסמך מדיניות זה נכתב בהתאם לדרישות שמוגדרות במדריך.

הגרסה הנוכחית של המסמך, אשר נמצאת במשרדו של ממונה הגנת הסייבר, זמינה לכל צוות העובדים. היא אינה כוללת מידע חשאי וניתן להפיץ אותה לגורמים חיצוניים רלוונטיים.

מדיניות אבטחת מידע זו אושרה בידי ההנהלה והופצה על בסיס ניהול גרסאות. היא מאושרת בחתימתו של סמנכ"ל משרד הכלכלה והתעשייה.

_____ _____

חתימה של מנכ"ל משרד הכלכלה והתעשייה תאריך