נוהל זה הותר לעיון על פי חוק חופש המידע

נהלי סמפכ"ל	פרק: **יחב"ם**	תת-פרק: **ביטחון מידע**	מספר: **04.01.08**

תאריך פרסום: **31/10/2021**	שם: **תדרוך אבטחת מידע במשטרת ישראל**
תאריך תחילה: **31/10/2021**	
תאריך ביטול:	
נוסח: **3**	

1. כללי

א. אנשי משטרה (שוטרים ואזרחים המועסקים במשטרת ישראל) הנחשפים למידע מסווג ו/או מחזיקים במידע מסווג, נדרשים להקפיד על כללים שונים לטיפול ראוי והולם במידע זה, במטרה למנוע דלף מידע לגורמים בלתי מורשים.

ב. לצורך כך נדרש מערך יחב"ם לבצע פעולות להעלאת רמת המודעות בקרב אנשי המשטרה, למניעת סיכונים בתחום אבטחת מידע, ולדרכי הפעולה הנכונות למזעור הסיכונים הללו, בהתאם לנהלי אבטחת המידע של יחב"ם.

ג. אחת הדרכים המרכזיות להשגת מטרה זו היא ביצוע תדרוך אבטחת מידע המבוצע ע"י קב"ט (נספח א) .

2. המטרה

הגדרת תוכן, תדירות ושיטות ביצוע תדרוך אבטחת מידע לאנשי משטרת ישראל ע"י הקב"ט.

3. השיטה ופירוט השיטה

א. <u>תדרוכי אבטחת מידע במשטרת ישראל יבוצעו בשלושה רבדים מרכזיים</u>:

1) **תדרוך תקופתי** – תדרוך אבטחת מידע המתבצע אחת לחמש שנים לכלל השוטרים / האזרחים המועסקים ע"י משטרת ישראל ומשמשים בתפקידים המסווגים ברמת "רז מועדף" (מקביל ל"סודי") ומעלה, לרבות יועצים, ספקים ועובדי חברות קבלניות. תדרוך תקופתי זה יכול להתבצע במתכונת של תדרוך אישי או תדרוך קבוצתי.

2) **תדרוך תקופתי "קרא וחתום"** – תדרוך אבטחת מידע המתבצע אחת לשנתיים לשוטרים / אזרחים המועסקים ע"י משטרת ישראל ומשמשים בתפקידים המסווגים ברמת "רז" (מקביל ל"שמור"), לרבות יועצים, ספקים, מאבטחים, אנשי תחזוקה ועובדי חברות קבלניות. באחריות הקב"ט המבצע את התדרוך בשיטת "קרא וחתום" לוודא כי ניתן מענה לכל השאלות של השוטר / האזרח העובר את התדרוך בטרם חתימתו.

3) **תדרוך אבטחת מידע מיוחד** – תדרוך אבטחת מידע המתבצע לשוטר / אזרח המועסק ע"י משטרת ישראל ומשמש בתפקיד המסווג ברמת "רז מועדף" ומעלה במקרים האלה:

א) בתחילת תפקיד ובסיום שירות / העסקה במשטרת ישראל;

ב) לקראת נסיעה לחו"ל במסגרת תפקיד, יבוצע לכלל השוטרים והאזרחים המועסקים ע"י משטרת ישראל ומשמשים בתפקידים המסווגים ברמת "רז מועדף" ומעלה;

ג) לקראת נסיעה לחו"ל שלא במסגרת תפקיד, ליעדים המחייבים ביצוע תדרוך אבטחת מידע, יבוצע לכל שוטר / אזרח המועסק ע"י משטרת ישראל שנסיעתו אושרה ע"י מפקד בכיר בדרגת נצ"מ ומעלה, בכפוף לביצוע תדרוך אבטחת מידע ע"י קב"ט;

ד) בכל מקרה אחר המחייב תדרוך אבטחת מידע, בהתאם לשיקולי הקב"ט;

ב. <u>פעולות קב"ט לקראת ביצוע תדרוך אבטחת מידע</u>:

1) הקב"ט יוודא את עדכניות רשימת השוטרים / האזרחים הנדרשים לעבור את התדרוך;

2) הקב"ט יקבע את מתכונת ואת מועד התדרוך, בהתאם לתוכנית העבודה השנתית שלו ויוציא זימונים לשוטרים / האזרחים הרלוונטיים;

3) הקב"ט ינהל יומן תדרוכי אבטחת מידע פיזי / ממוחשב;

4) הקב"ט יוודא את עדכניות התכנים ורלוונטיות הנושאים לתדרוך אבטחת מידע;

ג. <u>פעולות קב"ט לאחר ביצוע תדרוך אבטחת מידע</u>:

1) הקב"ט יחתים את המתודרך על טופס ביצוע תדרוך אבטחת מידע. הטופס החתום יישמר במשרד הקב"ט;

2) הקב"ט יתעד את דבר ביצוע תדרוך אבטחת המידע ביומן תדרוכי אבטחת מידע ויעביר דיווח כמותי שנתי ליחב"ם/ חו' אבטחת מידע;

ד. הנושאים שייכללו בתדרוך אבטחת מידע (למעט תדרוך לקראת נסיעה לחו"ל):

1) בסיס החוק המחייב שמירת סוד וקובע סנקציות לצדו;
2) האיומים עימם מתמודדת משטרת ישראל וגורמי איום בהיבטי ביטחון מידע;
3) האבטחה הפיזית של סביבת העבודה בהיבטי אבטחת מידע;
4) הכללים לשמירת סודיות ומידור;
5) כללי שימוש במערכות המידע ובמאגרי המידע המשטרתיים;
6) הכללים לסיווג המידע;
7) הכללים לאחסון מידע פיזי וממוחשב, בהתאם לרמת הסיווג שנקבעה לו;
8) הכללים להעברת מידע פיזי וממוחשב, בהתאם לרמת הסיווג שנקבעה לו;
9) הכללים להשמדת מידע מסווג;
10) כללי עבודה עם מחשבים משטרתיים (נייחים, ניידים, סלולריים);
11) כללי שימוש באמצעי מדיה נתיקה;
12) כללי שימוש ברשתות חברתיות ובפורומים ברשת האינטרנט;
13) כללי שימוש במכשירי קשר מוצפנים משטרתיים;
14) כללי נדב"ר ברשת הקשר המשטרתית;

ה. הנושאים שייכללו בתדרוך אבטחת מידע לקראת נסיעה לחו"ל:

1) סקירת האיומים הנשקפים לישראלים / אנשי ביטחון ישראלים בחו"ל בכלל וביעד הספציפי בפרט;
2) דגשים כלליים לקראת נסיעה לחו"ל;
3) איומים בתחום ניסיונות גיוס והפעלה ע"י גורמי ביון וביטחון זרים;
4) איומים בתחום אבטחת מידע לבעלי תפקיד מסווגים;
5) כללי שימוש במידע משטרתי מסווג בחו"ל (בתדרוך לקראת נסיעה במסגרת תפקיד בלבד);
6) התנהגות מומלצת בטיסה;
7) דגשים בתחום שמירת הביטחון האישי, התנהגות כללית והתנהגות למניעת חטיפה במקומות ציבוריים ובבתי מלון בחו"ל;
8) דרכי פעולה אפשריות במצבי חרום בחו"ל;
9) הבהרת חובת דיווח לקב"ט במקרים של ניסיונות גיוס והפעלה ו/או אירועים חריגים / חשודים שהתרחשו במהלך שהות בחו"ל;

4. תחומי אחריות

א. האחריות לביצוע הנוהל זה – כל קב"ט מחוזי/ אגפי/ יחידתי.

ב. האחריות לעדכון הנוהל – יחב"ם / חו' ביטחון מידע.

נספח א'

הצהרה לאחר קבלת תדרוך אבטחת מידע

אני הח"מ מצהיר/ה בזאת שעברתי תדרוך אבטחת מידע שכלל את התכנים המפורטים במסמך שלהלן ושקראתי בעיון רב את ההנחיות שלהלן ואני מתחייב/ת לשמור על הכללים וההוראות בדבר שמירת סודיות ואבטחת מידע.

1. אבטחת ציוד, אמצעים ומדיה ממוכנת

א. יש לשמור את המידע והאמצעים המסווגים על פי רמות הסיווג שלהם.

ב. אין להוציא מידע מסווג אל מחוץ למתקני משטרה לרבות – מסמך, ניירת, מדיה מגנטית לסוגיה או אמצעי המכיל מידע מסווג או שמוגדר כמסווג, לבית או למקום פרטי. כל הוצאה אל מחוץ למתקן משטרתי של מידע שהוגדר ברמת סיווג "שמור" ומעלה, לרבות מסמך פיזי מודפס, מדיה מגנטית או אמצעי ממוחשב המכיל מידע מסווג כאמור, תהיה בהתאם לנהלים והנחיות יחב"ם ובכפוף לאישור מפקדים.

ג. ככלל, אין לחבר מדיה נתיקה למחשבי רשת טלי. העברת מידע לרשת טלי וממנה תיעשה באמצעות עמדות מע' הלבנה / השחרה של משטרת ישראל.

ד. אין לשכפל / לצלם / להעתיק מידע או מסמך ברמת סיווג "סודי ביותר".

ה. אין להכניס מחשבים פרטיים אזרחיים למתקני המשטרה או לחברם לאמצעים משטרתיים ו/או לרשתות תקשורת משטרתיות (טלי / מירי). הכנסת אמצעי מחשוב פרטיים למתקן משטרתי תהיה בכפוף לאישור פרטני מיוחד של הקב"ט הנוגע.

ו. איסור על הוצאת מחשבים ניידים משטרתיים שלא באישור הגורמים המוסמכים, ואבטחתם, על פי נוהלי אבטחת המידע במחשבים נישאים. חובת דיווח מיידית על אובדן/ גניבת מחשב נייד.

ז. השימוש במערכות ומאגרי המידע המשטרתיים יהיה לצורך ביצוע תפקיד בלבד ובהתאם להנחיות ונוהלי יחב"ם .

ח. חל איסור על שימוש במערכות המידע המשטרתי והוצאת מידע ממערכות אלה לצרכים הפרטיים, שלך או של אחרים ושלא לצורכי עבודת המשטרה, לרבות לצורך מילוי פרטים אישיים שלך או של בני משפחתך או של אחרים בטפסים השונים.

ט. שם המשתמש, הסיסמא וסיסמת OTP המאפשרים כניסה לרשת טלי הינם אישיים וחל איסור להעבירם לשום גורם נוסף.

י. חובת נעילת מחשב בעת יציאה מהחדר לזמן קצר ויציאה מהרשת (פעולת "צא") בסוף יום העבודה.

יא. חובת נעילת דלתות של מתחמים/ משרדים בעת יציאת העובד האחרון מהמקום. אין להשאיר חדרים פתוחים ללא השגחה.

תאריך _____ חתימה _____

2. <u>טיפול במידע</u>

א. אין להעביר מידע משטרתי מסווג (לרבות בעל פה, בכתב, קובץ או בכל דרך אחרת) לידי גורם שאינו מורשה לכך ושלא לצרכי העבודה.

ב. שמירת כלל הקבצים במחשבים תהיה על כוני הרשת בלבד(Z, K, G ועוד) .

ג. חל איסור להעלות מידע הנוגע לתפקידך במשטרה או מידע משטרתי מקצועי ברשתות החברתיות או בכל פורום ותכתובת באינטרנט, שיש בהם משום חשיפה לשיטות עבודה, לצנעת הפרט או לבעלי תפקידים ייחודיים .

ד. חל איסור על שימוש בתווך אינטרנטי להעברת מידע מסווג (למעט באמצעות "כספות וירטואליות" ועל פי אישור קונקרטי של יחב"ם).

ה. הקפדה על הפרדה בין אשפה מסווגת המיועדת לגריסה לבין אשפה לא מסווגת.

ו. השמדת מדיה מגנטית המכילה מידע מסווג וכן גריסת מסמכים מסווגים שאין בהם עוד שימוש תתבצע על ידי מחזיק המידע / המסמכים או על ידי מורשה מטעמו, בעל סיווג שאינו נמוך מסיווג המידע / המסמך הנגרס.

ז. חובת רישום סיווג תואם לכל מסמך, בהתאם לנוהל יחב"ם 04.01.01 "סיווג, אחסון, אבטחה, הפצה והשמת מידע משטרתי מסווג" .

ח. הקפדה בעת שימוש באמצעי תקשורת על התאמת סיווג התוכן לסיווג האמצעי והימנעות מפירוט מידע רגיש שאינו תואם את רמת סיווג אמצעי התקשורת.

ט. איסור אגירת מידע מסווג בטלפונים סלולאריים, לרבות העלאת מידע מסווג בצורת תמונה, סרט, או הקלטה, שימוש באפשרויות המסרונים והזיכרון לשמירת מידע מסווג, ציון יחידות ותפקידים מסווגים בספר הטלפונים.

י. שימוש בטלפונים ניידים לצורך טיפול במידע מסווג יהיה בהתאם לפקודת המטא"ר מספר 14.02.01 "השימוש בטלפון סלולארי אישי על ידי שוטרים לצורכי עבודה" והנחיות יחב"ם בלבד (לצורך שימוש ביישומים משטרתיים, העברת מידע מסווג באמצעות מע' מיסרונט ושימוש לצורך תיעוד זירת עבירה).

יא. איסור על שימוש באפליקציות סלולאריות אזרחיות להעברת מסרים מידיים לצורך העברת מידע משטרתי מסווג.

3. <u>כניסה למתקני משטרה</u>

א. כניסה למתקן רק לשוטרים/אזרחים המועסקים ע"י משטרת ישראל באישור הפיקוד המקומי , או למבקרים חיצוניים אשר הוזמנו ע"י גורם משטרתי מקומי שהסדיר מראש אישור כניסה עבורם.

ב. חובת ליווי צמוד של אורחים / גורמי חוץ המגיעים למתקן משטרתי / מתחם משטרתי המצוי במתקן אזרחי מרגע הכניסה ועד ליציאה והקפדה כי הגורם המבקר ימצא רק במקומות הנדרשים לצורך ביצוע משימתם ובהתאם לאישור הכנסה שקיבלו .

תאריך _____ חתימה _____

ג. חובת בדיקת זהות גורמים זרים לא מוכרים בתוך מתקן משטרתי/מתחם משטרתי במתקן אזרחי ובמקרה הצורך - עיכובם והעברתם להמשך טיפול הגורם המשטרתי המתאים במקרה של נסיבות מחשידות.

ד. מניעת כניסת גורמים שאינם מורשים ובכלל זה שוטרים שאינם מורשים למתחמים מסווגים/ ממודרים.

ה. פיקוח / ליווי צמוד לפועלים ועובדי קבלן העובדים במתחמים משטרתיים ואיסור השארת עובדי ניקיון ללא פיקוח צמוד בעת כניסתם לחדרי עבודה.

ו. מניעת גישת אורחים ו/או גורמי חוץ למערכות המחשב, למאגרי המידע ומניעת חשיפתם לכל מידע / מסמך המכיל מידע מסווג החורג ממטרת הגעתו של אותו גורם חיצוני למתקן משטרתי.

4. חובת מילוי הנחיות יחב"ם המופצות מעת לעת כהודעת ארגון במשטרת ישראל.

5. <u>הובא לידיעתי הבסיס החוקי לחובות החלות עלי בשמירת סודיות המידע המסווג המגיע אלי מתוקף עבודתי במשטרה ובכלל זה :</u>

א. **<u>חוק העונשין תשל"ז- 1977, ס' 117 (א) – סודות רשמיים גילוי בהפרת חובה</u>** עובד הציבור שמסר, ללא סמכות כדין, ידיעה שהגיעה אליו בתוקף תפקידו, לאדם שלא היה מוסמך לקבלה, וכן מי שהגיעה אליו ידיעה בתוקף תפקידו כעובד הציבור, ולאחר שחדל מהיות עובד הציבור מסרה, ללא סמכות כדין, לאדם שלא היה מוסמך לקבלה – דינו מאסר 3 שנים.

ב. **<u>חוק העונשין תשל"ז – 1977 ס' 117 (ב) – שמירת ידיעה</u>**
עובד הציבור שהתרשל בשמירת ידיעה שהגיעה אליו בתוקף תפקידו או שעשה מעשה שיש בו כדי לסכן ביטחונה של ידיעה כאמור – דינו מאסר שנה.

ג. **<u>חוק הגנת הפרטיות, התשמ"א-1981</u>**
לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, אלא לצורך ביצוע עבודתו או לביצוע חוק זה. המפר הוראות סעיף זה, דינו - מאסר 5 שנים.

- **אין בנושאים ובדגשים שלעיל כדי להחליף את החובה להכיר את כלל נהלי בטחון המידע של משטרת ישראל ואשר מופיעים במניפ"ה/נהלים/סמפכ"ל/יחב"ם/ביטחון מידע.**

אני מצהיר/ ה בזאת, כי קראתי והבנתי במלואם את עמודים 1-3 בתדרוך ביטחון מידע תקופתי לעובד וכי אמלא אחר כל הכללים וההנחיות המפורטים בהם.

שם פרטי _____ שם משפחה _____ ת.ז _____

תאריך _____ חתימה _____