נוהל זה הינו נוסח חלקי שהותר לעיון על פי חוק חופש המידע

נהלי סמפכ"ל	פרק: **יחב"ם**	תת-פרק: **ביטחון מידע**	מספר: **04.01.03**

תאריך פרסום: **04/08/2020**	שם: **שימוש במערכת המיסרונט להעברת מידע משטרתי מסווג**
תאריך תחילה: **24/03/2020**	
תאריך ביטול:	
נוסח: **1**	

1. **<u>מטרת הנוהל:</u>**

קביעת כללים מנחים לשימוש במיסרונט להעברת מידע משטרתי מסווג, על מנת למזער סיכוני דלף מידע מסווג ולמנוע פגיעה בפעילות משטרת ישראל בשגרה ובחרום כתוצאה מדלף מידע מסווג.

2. **<u>כללי:</u>**

מערכת "מיסרונט" פותחה ע"י אטו"ב, על מנת לספק מענה זמין, נוח ומאובטח לצרכים הבאים של משטרת ישראל:

א. הפצת דיווחים מבצעיים, הנחיות פיקוד, עדכונים, הודעות מנהליות וצרופות של קבצי מידע לגורמי משטרה רלוונטיים ולגורמי שת"פ מורשים.

ב. יצירת ערוץ זמין ומאובטח לשיח מפקדים.

ג. העברת מידע מסווג ברמת סיווג "סודי" (כולל) למורשים ויצירת סביבת עבודה מאובטחת ליחידות המיוחדות ולמגזרים המסווגים של משטרת ישראל.

ד. יצירת חלופה מאובטחת לאפליקציות אזרחיות להעברת מסרים מידיים (WhatsApp, Telegram ודומות אחרות), במטרה לאפשר העברת מידע מסווג, ולמזער סיכונים לדלף מידע משטרתי / ביטחוני מסווג ורגיש.

ה. יצירת קבוצות משתמשים יחידתיות/מגזריות/מקצועיות לצורך שיתוף מידע והתכתבות בין המשתמשים.

3. **<u>הגדרות:</u>**

"מערכת מיסרונט" – מערכת משטרתית להפצת הודעות מידיות שפותחה במשטרת ישראל. המערכת משלבת בתוכה אפליקציה סלולרית ייחודית המאפשרת העברת מסרים מידיים (דיווחים, הודעות, קבצים) והתכתבות בין המשתמשים. כמו כן, המערכת מאפשרת הפצת הודעות כתובות וקוליות מעמדות מחשב ברשת "טלי" המשטרתית למשתמשי הקצה באפליקציה הסלולרית (מיסרונט). המערכת מאפשרת העברת הודעות רגילות שמכילות מידע עד רמת סיווג "שמור" (כולל) וכן העברת הודעות "מאובטחות" שמכילות מידע עד רמת סיווג "סודי" (כולל).

"היחידה לביטחון מידע במשטרת ישראל (יחב"מ)" – היחידה האחראית על קביעת מדיניות ביטחון המידע וביצוע התאמה תעסוקתית במשטרת ישראל.

"מידע" – נתון, מסמך ו/או תוכן בכל נושא, לרבות נושאים מודיעיניים, מקצועיים, מנהלתיים ופרטיים.

"סיווג של מידע" – קביעת ערכו הביטחוני ו/או המשטרתי של מידע, בהתאם למידת הנזק העלול להיגרם לציבור כולו או לפרטיות ולצנעת חייו של אדם מן הציבור או לעבודת המשטרה, כתוצאה מחשיפת המידע/המסמך לגורם בלתי מוסמך. הסיווגים הקיימים הם: "בלמ"ס", "שמור", "סודי", "סודי ביותר", "סוד מיוחד".

"מידע/מסמך מסווג" – מידע או מסמך שלגביו נקבע הסיווג, **מרמת "שמור" ועד "סוד מיוחד".**

"גורם מוסמך" – גורם משטרתי או חוץ משטרתי, הרשאי מתוקף תפקידו לקבל מידע/מסמך מסווג לצורך מילוי תפקידו.

"גורם בלתי מוסמך" – כל גורם שאינו מוסמך מתוקף תפקידו לקבל מידע/מסמך מסווג.

4. עקרונות ביטחון מידע:

א. חשיפת מידע מסווג, לרבות מידע מודיעיני וחקירתי, שיטות עבודה, אמצעים משטרתיים ונתונים אישיים של אזרחים ושוטרים, בפני גורמי בלתי מוסמכים, עלולה להביא לדלף מידע ולגרום לפגיעה בעבודת המשטרה, בביטחון הציבור, בשלומו ובפרטיותו .

ב. שמירה על נוהלי ביטחון מידע והקפדה על מידור, ימנעו הגעת מידע מסווג לידי גורמים בלתי מוסמכים.

ג. היחידה לביטחון מידע (יחב"מ) פועלת בשיתוף פעולה הדוק עם אטו"ב אשר מעניק מעטפת ומענה טכנולוגי, על מנת לצמצם ככל הניתן את הסיכון לפגיעה בסודיות, שלמות וזמינות מידע משטרתי ומידע אישי מסווג.

ד. מידע משטרתי מסווג יופץ רק לגורמים בתוך הארגון או מחוצה לו שהוסמכו לקבלו לצורך ביצוע תפקידם.

ה. האחראי ליצירת מידע או מסמך, מחויב להקפיד על מידור תוכנו מגורמים שאינם מוסמכים לקבלו, בארגון ומחוצה לו.

5. השיטה:

א. במערכת מיסרונט יועבר מידע משטרתי בהתאם לכללים הבאים:

1) הודעות רגילות, לרבות צרופות של קבצי מידע שונים (PDF, תמונות, קבצי שמע, הודעות קוליות וכל סוג אחר של קבצים, בהתאם להתפתות הטכנולוגית ושדרוג המערכת) – עד רמת סיווג "שמור" (כולל).

2) הודעות קוליות רגילות (מיסרונט קולי) – עד רמת סיווג "שמור" (כולל).

3) הודעה מאובטחת אשר מחייבת הקשת סיסמה אישית של הנמען (לרבות הודעה עם צרופה והודעה קולית) – עד רמת סיווג "סודי" (כולל).

ב. בנוגע למידע שמקורו באחד הגופים במערכת הביטחון, יש להיצמד לרמת הסיווג שנקבע למידע ע"י מחבר המידע באותו גוף ביטחוני וניתן להוריד את רמת הסיווג רק באישורו.

ג. חל איסור להעתיק ו/או להעביר כל מידע מסווג שהתקבל באמצעות הודעות מיסרונט (גוף הודעה, תוכן הודעה, קבצים מצורפים) בכל דרך ובכל אמצעי.

ד. חל איסור לחשוף תוכן של הודעות מיסרונט לגורמים בלתי מוסמכים.

ה. איש משטרה אשר מעביר באמצעות מע' מיסרונט מידע מסווג לגורם חוץ שמוסמך לקבלו, מחובתו להנחות גורם חוץ זה בנוגע לכללי ביטחון המידע שחלים עליו, דהיינו – איסור העתקה המידע ואיסור העברת המידע לכל גורם אחר שאינו מוסמך לקבלו.

ו. בהודעות מיסרונט לקבוצות תפוצה רחבות – יש לערוך בדיקה עתית בנוגע לעדכניות רשימת התפוצה ובעלי התפקידים המצויים בה. ריבוי מכותבים והימצאות בעלי תפקידים שאינם רלוונטיים למידע, או כאלה שעזבו את החייל עשוי להביא לדלף מידע מסווג ורגיש.

ז. מכשיר סלולרי שנמסר לתיקון, מועבר לבן משפחה, נמכר או אמור להגיע מכל סיבה אחרת ובכל דרך לגורם שאינו מוסמך להיחשף למידע משטרתי מסווג, יש להסיר ממנו את מזהה המכשיר ואת כלל האפליקציות המשטרתיות, בדגש על המיסרונט.

6. <u>עקרונות סיווג המידע</u>

א. רמת סיווג של מידע נקבעת בהתאם למידת הנזק העלול להיגרם כתוצאה מחשיפת תוכנו למי שאינו הוסמך לכך.

ב. להלן פירוט רמות סיווג המידע המשטרתי והקריטריונים לקביעת רמות הסיווג כאמור:

רמת סיווג	הקריטריונים להגדרת רמת סיווג לפי מידת הנזק
"בלמ"ס" (בלתי מסווג)	מידע אשר חשיפת תוכנו לגורם כלשהו לא תגרום כל נזק.
"שמור"	מידע אשר חשיפת תוכנו לגורמים בלתי מוסמכים עלולה לגרום נזק לביטחון הציבור, לפעילות תקינה של מ"י או מערכותיה או לניהולה התקין או לפגוע בפרטיותו של אזרח או שוטר.

רמת סיווג	הקריטריונים להגדרת רמת סיווג לפי מידת הנזק
"סודי"	מידע שחשיפת תוכנו לגורמים בלתי מוסמכים עלולה לגרום נזק חמור לביטחון הציבור, לפעילות תקינה של מ"י או לניהולה התקין או חשיפתו לידי גורמים בלתי מוסמכים עלולה לגרום לפגיעה בחיי אדם או לפגיעה ממשית בצנעת הפרט.
"סודי ביותר"	מידע אשר חשיפת תוכנו לגורמים בלתי מוסמכים עלולה לגרום נזק חמור מאד וממושך לביטחון הציבור ולפעילות תקינה של מ"י, פגיעה בדרכי הפעולה והניהול התקין של המשטרה וכן יכולה להביא בעליל לפגיעה בחיי אדם (מקורות, סוכנים משטרתיים וכיו"ב) או לפגיעה קשה וחמורה בצנעת הפרט.

7. <u>חיבור גורמי חוץ למערכת מיסרונט</u>

א. חיבור גורמי חוץ למערכת מיסרונט משטרתית ייעשה עפ"י מדיניות כפי שנקבעה ע"י אג"מ/חט' המבצעים, אשר גובשה יחד עם יחב"מ ובהתאם לקווים המנחים שלהלן:

1) גורמי חוץ לא יחוברו לקבוצות דיווח משטרתיות מבצעיות, לא ברמת המחוזות ולא ברמה הארצית, למעט חריגים בודדים, עפ"י החלטת רמ"ח מבצעים ואישור יחב"מ.

2) באחריות יחידות הטכנולוגיה במחוזות, את"ן, להב, מג"ב ובמב"צ ברמה הארצית:

א) ליצור קבוצות דיווח ייעודיות עבור גורמי חוץ שייקראו "גורמי שת"פ".

ב) להעביר את גורמי החוץ הקיימים שמחוברים לקבוצות מחוזיות/קבוצת הודעות פיקוד ארצית במיסרונט, לקבוצות החדשות של גורמי שת"פ כאמור.

3) בחינת הצורך המבצעי בחיבור גורמי חוץ לקבוצות גורמי שת"פ במיסרונט ברמת מחוז/מג"ב תיעשה ע"י אג"מ המחוז הנוגע/מג"ב. בחינת הצורך המבצעי ברמה הארצית תיעשה ע"י מב"צ.

4) תינתן עדיפות ברורה לחיבור משל"טים/מוקדים/חמ"לים ומרכזי הפעלה של גורמי חוץ על פני בעלי תפקידים יחידים, לקבוצות גורמי שת"פ בלבד, כפי שצוין בסעיף 6א'.

5) אישור גורמי חוץ ברמת מחוז/ מג"ב יינתן ע"י קב"ט המחוז/מג"ב הנוגע. אישור גורמי חוץ ברמה הארצית יינתן ע"י יחב"מ.

6) מקרים חריגים יידונו בפני רמ"ח מבצעים אג"מ.

7) באחריות מנהל מערכת בכל מצודה מחוז/ מג"ב/ להב/ מצודה ארצית:

א) חיבור גורמי חוץ מאושרים, לאחר אישור יחב"מ וסיום הטיפול של הטכנולוגיות.

ב) הבהרה לנציג גורם חוץ מורשה כי חל איסור להעביר את המידע שהועבר אליו ממשטרת ישראל לגורמים שאינם מוסמכים, לרבות צילום מסך, הפצת המידע באמצעות אפליקציות סלולריות כגון WhatsApp ודומות לה, רשתות חברתיות ובכל דרך אחרת.

ב. באג"מ במחוזות / מג"ב ובמב"צ ברמה הארצית ינוהל תיעוד מסודר של הבקשות לחיבור גורמי חוץ למיסרונט, לרבות התייחסות גורם אג"מ בכיר (ק' אג"מ מחוזי/רע"ן מבצעים) וינוהל מעקב אחרי תחלופת בעלי התפקידים אשר חוברו למיסרונט בקרב גורמי חוץ.

8. <u>דלף מידע מסווג ממערכת המיסרונט:</u>

א. היה והתברר לגורם משטרתי או גורם מוסמך חוץ משטרתי, כי המידע שהועבר באמצעות מע' מיסרונט דלף לגורמים שאינם מוסמכים לקבלו, **ידווח על כך באופן מיידי** לראש יחב"מ או לקב"ט ביחידתו/קב"ט בגוף אליו משתייך גורם חוץ מוסמך.

ב. בכל מקרה של דלף מידע ממערכת מיסרונט תקיים יחב"מ הערכת נזק ותחליט בתום התהליך על נקיטת צעדים נוספים במידת הצורך.

9. מעקב וביקורת:

א. אחריות ליישום הנוהל – כל מפקד בדרגתו.

ב. אחריות לעדכון הנוהל – יחב"מ.