נוהל זה הותר לעיון על פי חוק חופש המידע

נהלי סמפכ"ל	פרק: **יחב"ם**	תת-פרק: **ביטחון מידע**	מספר: **04.01.13**

תאריך פרסום: **18/08/2020**	שם: **היבטי ביטחון מידע באבטחת מחשבים משטרתיים**
תאריך תחילה: **18/08/2020**	
תאריך ביטול:	
נוסח: **1**	

**** מס' נוהל ישן 03.345.622

כללי

מחשבים משטרתיים מהווים אמצעי גישה להמידע מסווג ורגיש המצוי במערכות ובמאגרי המידע של משטרת ישראל. חשיפת המידע ממערכות ומאגרי המידע של משטרת ישראל לגורמים בלתי מורשים עלולה לגרום נזק ברמות חומרה שונות, למשטרת ישראל, למדינת ישראל, לציבור כולו ו/או לאדם מן הציבור.

מטרת הנוהל

לקבוע עקרונות וקווים מנחים של יחב"ם באבטחת מחשבים משטרתיים.

הגדרות

א. **מחשב משטרתי** – מחשב נייח או נייד שנרכש, נבדק ואושר לשימוש ע"י אטו"ב מ"י, אשר המעבד או המאחסן מידע משטרתי ו/או מחובר לרשת תקשורת נתונים של משטרת שיראל.

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

ג. **מסמך** – מצע מידע המאוחסן באופן כלשהו (פיזי / ממוחשב / מגנטי / אלקטרוני), לרבות כל רישום שנעשה בכתב יד, בהקלדה, בהקלטה, בצילום או באמצעי טכני אחר, שממנו הופק אחד מאלה: נייר מודפס או כתוב בכתב יד, קובץ במחשב, קלטת של תמונה, קלטת של קול, תצלום, מפה, תרשים, תבליט, סרט צילום, סרט מגנטי,

תקליטור, דיסק, פלט מחשב או כל תוצר אחר של רישום שנעשה באמצעי טכני, בין שהמידע בהם קריא ובין שאינו קריא, בין שהמידע ניתן לפענוח ובין שלא, בין שהמידע מלא ובין שהוא פגום או אינו מושלם.

ד. **מדיה (אופטית, מגנטית ואחרת)** – התקן המיועד לאחסון מידע ממוחשב, כגון: דיסק קשיח פנימי או חיצוני, קלטות, דיסק און קי/דיסק נשלף, וכד'.

ה. **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".

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

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

<u>השיטה</u>

א. עקרונות הטיפול במידע מסווג אשר נקבעו בנוהל יחב"מ **"סיווג, אחסון, אבטחה, הפצה והשמדת מידע משטרתי מסווג"**, חלים גם על הטיפול במידע מסווג ממוחשב.

ב. ככלל, במשרדים המשמשים מספר רב של שוטרים, כגון: חדרי תדרוך סיירים וכו' אין להציב מחשבים משטרתיים המחוברים לרשת המשטרתית. חדרי דיונים בהם נדרשת התקנת עמדת מחשב המחוברת לרשת המשטרתית יהיו נעולים בכל עת שבהם אין נוכחות של שוטרים.

ג. חל איסור להכניס ליחידות משטרה מחשבים פרטיים, לרבות מחשבים נייחים, ניידים, מחשבי לוח וכל ציוד מחשוב פרטי, למעט טלפונים סלולאריים.

ד. למחשבים המשטרתיים לא יוספו ולא יחוברו רכיבי תקשורת אזרחיים, בדגש על רכיבי תקשורת אלחוטיים וטלפונים סלולאריים. חל איסור להתקין במחשבים משטרתיים תוכנות שלא נבדקו ואושרו ע"י אטו"ב.

ה. סיסמת הכניסה למחשב משטרתי הינה אישית ולא תועבר לאחרים. הסיסמא לא תישמר במקום גלוי ולא תודבק למחשבים ולציוד המחשוב.

ו. ככלל, במצב כיום, כל גישה למחשב משטרתי מחייבת שימוש בסיסמא (סיסמא אישית / OTP והשילוב בין השתיים). בנוגע לסיסמא האישית, איכות הסיסמא, הרכב התווים האקראי שלה ואי חשיפתה לעובדים אחרים מסייעים לאי-חשיפתה לבלתי מורשים. על כן, יש לבחור סיסמא שלא תיהיה קלה לניחוש ולא מורכבת מהפרטים האישיים של בעל הסיסמא.

ז. בכל מקרה של חשש לחשיפת סיסמא אישית לגורם כשלהו מלבד בעל הסיסמא, יש לדווח על כך באופן מידי לקב"ט הרלוונטי ולהחליף את הסיסמא האישית באמצעות ק' מחשוב / מרכז שירות אטו"ב.

ח. מחשבים משטרתיים המחוברים לרשת המשטרתית לא יחוברו לרשת האינטרנט ו/או לכל רשת חיצונית אחרת. מחשבים אזרחיים לא יחוברו לרשת המשטרתית.

ט. מדפסות המחוברות לרשת המשטרתית וכן מדפסות המחוברות באופן מקומי למחשבים

משטרתיים לא יחוברו במקביל למחשבים ברשת חיצונית כלשהי.

י. דיסקים קשיחים משטרתיים תקולים, רכיבים אוגרי מידע שפורקו ממחשבים משטרתיים וממכונות הצילום ביחידות משטרה, אמצעי מדיה נתיקה תקולים המכילים מידע משטרתי ותקליטורים המיועדים להשמדה יועברו לגריסה / התכה.

א. טיפול במחשבי משטרתיים תקולים ייעשה בהתאם לקבוע בנוהל יחב"מ "**טיפול בתקלות חומרה**". ככלל, במידה והטיפול במחשב משטרתי תקול יתבצע ע"י נותן שירות חיצוני, הזמנת נותני שירות חיצוניים לטיפול בתקלות תעשה ע"י גורמי המערך הטכנולוגי במשטרת ישראל בלבד. יש ללוות את נותן השירות החיצוני במהלך שהותו במתקן משטרתי. יש לוודא שנותן השרות החיצוני לא ישאר לבדו עם המחשב ולא יפרק כל רכיב אוגר מידע מהמחשב.

יא. בכלל המחשבים המשטרתיים יותקנו אמצעי אבטחה לוגיים ו/או פיזיים אשר אושרו ע"י אטו"ב.

יב. בכלל המחשבים המשטרתיים יותקן יישום אנטי-ווירוס מעודכן ומאושר ע"י אטו"ב.

יג. כלל מסמכי העבודה הממוחשבים יאוחסנו בתיקיות בכווני רשת מרוחקים ולא בכוננים המקומיים במחשב.

ב. ככלל כל גישה למחשב מחייבת בשימוש בסיסמא אישית ובאימות מרכזי. איכות הסיסמא, הרכב התווים האקראי שלה ואי חשיפתה לעובדים אחרים מהווים את המחסום העיקרי בפני משתמשים לא מורשים. על כן, יש לקבוע את הסיסמא, כך שלא תיהיה קלה לניחוש ולא מורכבת מהפרטים האישיים של בעל הסיסמא.

ג. יש לוודא הפעלת "שומר מסך" לאחר פרק זמן שייקבע ע"י אטו"ב של היעדר כל פעילות במחשב, בכל מחשב משטרתי.

ד. השימוש במדיה נתיקה במחשב משטרתי לצורך ההוצאה או ההכנסה של מידע, יהיה ייעשה ע"י מורשים בלבד ולאחר בדיקת האמצעי הנתיק וקבצעי המידע באמצעות מע' הלבנה / השחרה.

ה. יש לסמן את המחשבים המשטרתיים בהתאם לרשת תקשורת נתונים אליה הם מחוברים (רשת משטרתית, רשת אינטרנט, רשת צה"ל וכיו"ב).

ט. חל איסור מוחלט לחבר מחשב משטרתי לרשת האינטרנט. חל איסור לחבר מחשב אינטרנט לרשת תקשורת נתונים משטרתית.

י. הכונן הקשיח של מחשב משטרתי יוצפן באמצעות תכנה מאושרת ע"י אטו"ב.

יא. יש להקפיד על נעילת מחשב משטרתי בכל עת של היעדר איוש עמדת מחשב / הפסקה ו/או כל מצב של היעדר פיקוח צמוד על המחשב, בדגש על סוף יום העבודה.

יב. במקרה של אובדן / גניבה של מחשב – חובה לדווח למפקד, לתחנת המשטרה הקרובה ולקב"ט הרלוונטי.

<u>תחומי אחריות</u>

א. אחריות ביצוע הנוהל

כלל השוטרים והאזרחים המועסקים במשטרת ישראל

ב. אחריות פיקוח ובקרה

יחב"ם

ג. אחריות לעדכניות הנוהל

יחב"ם / חו' ביטחון מידע

<u>תחולה</u>

הנוהל תקף החל מיום פרסומו