

## ניהול ואבטחת מידע אישי – 0317

### עיקרי הנוהל:

- לאור רגישותו הגבוהה של המידע האישי, ולנוכח המחויבות החוקית הנגזרת מחוק הגנת הפרטיות, התשמ"א-1981, מדרישות חוקיות ורגולטוריות רלוונטיות אחרות וממדיניות אבטחת המידע של האו"פ נוקטת האו"פ באמצעים שונים לניהול ואבטחת המידע.
- האו"פ רואה בחומרה פגיעה בפרטיות, שיש בה משום הפרת הוראות החוק להגנת הפרטיות, והוראות נוהל זה.
- ניהול ואבטחה של כלל מאגרי המידע באו"פ, המכילים מידע אישי יבוצעו על-ידי בעלי התפקידים, בהתאם לסמכויותיהם ותחומי אחריותם, כמפורט בנוהל, ובכלל זה הנחיות לגבי איסוף מידע, גישה למידע, תקינות המידע, מסירת מידע והגנה פיזית על מידע.
- ההנחיות החלות באשר לניהול ואבטחת מידע אישי תקפות לכל מדיה אפשרית המשמשת לאחסון, קרי, מאגרי המידע, אמצעי אחסון ניידים/נתיקים ומסמכים מודפסים.

### מטרות

- ליישם את קווי מדיניות אשר נקבעו באו"פ לניהול ואבטחת מידע אישי המאוחסן במאגרי האו"פ.
- להגדיר את מחויבות המנהלים והעובדים לשימוש נאות במידע אישי.

### הגדרות

- חוק הגנת הפרטיות, התשמ"א-1981** – חוק המסדיר את סוגיית הזכות לפרטיות ומגדיר פגיעה בפרטיות. החוק מתייחס גם למאגרי מידע אישי, לרבות ניהול מידע אישי ("החוק").
- מידע אישי** – מידע שיש חובה לשמור על חסונו במסגרת העבודה השוטפת באו"פ. מידע זה מוגדר בחוק וכולל את הפרטים והנתונים הבאים:
  - לגבי **עובד** – נתונים הנוגעים לענייניו הפרטיים ולצנעת חייו האישיים, לרבות שמו וכתובתו, מס' הזיהוי שלו, מצב בריאותו, מצבו המשפחתי, שרותו צבאי, נתונים הקשורים למצבו הכלכלי, לרבות, משכורתו, הלוואות שקיבל, פרטי חשבון בנק/כרטיס אשראי, וכן, נתונים הקשורים לתפקודו המקצועי, לרבות דוחות הערכה, חוות דעת ונושאי משמעת.
  - לגבי **סטודנט** – נתונים הנוגעים לענייניו הפרטיים ולצנעת חייו האישיים, לרבות שמו וכתובתו, מס' הזיהוי שלו, מצב בריאותו, מצבו המשפחתי, שרותו הצבאי, היותו אסיר, נתונים הקשורים למצבו הכלכלי, לרבות פרטי חשבון בנק/כרטיס אשראי, נתונים הקשורים ללימודיו, לרבות, קורסים נלמדים, ציוני קורסים ובחינות, נתוני בקשה למלגה או נתוני הענקת מלגה ונושאי משמעת.
  - לגבי **ספק** – נתונים הנוגעים לענייניו הפרטיים של ספק (או מי מעובדיו) לרבות דרכי קשר, מצבו הכלכלי של העסק שבבעלותו, פרטי חשבון בנק, חו"ד ועוד, למעט מידע שהוא נחלת הכלל.

## ניהול ואבטחת מידע אישי – 0317

- **מסמך חסוי** - מסמך אלקטרוני, טופס בכתב יד, או תדפיס שהופק ממאגרי המידע המכיל מידע אישי.
- **סטודנט** - לומד באו"פ במערך הלימודים האקדמי.
- **תלמיד** – לומד באו"פ בכל יחידה שאינה במערך הלימודים האקדמיים
- **יחידה** – גוף ארגוני (מינהל, מחלקה וכיו"ב) הממונה על תחום מסוים של פעילות אקדמית, חוץ אקדמית או מנהלית.
- **גורם חיצוני** – גוף המקושר עם האו"פ, ונדרש לממשקי עבודה מקוונים ואחרים בהקשר למידע אישי, דוגמת ספק שירותי מחשוב, ספק שירותי יעוץ, מוסד ציבורי, מרכז לימוד בניהול חיצוני, אגודת הסטודנטים.

### שיטה

1. עובד המטפל במידע אישי ינקוט משנה זהירות, ישמור על סודיות המידע ויהיה מודע לכך שגילוי ו/או חשיפה של מידע אישי עלולים לגרום לפגיעה בפרטיות, ובעקבות זאת לנזק ממשי לנשוא המידע.
  - 1.1 פגיעה בפרטיות, שיש בה משום הפרת הוראות החוק להגנת הפרטיות, עלולה להוות עבירה אזרחית ופלילית.
  - 1.2 עובד המגלה או חושף מידע אישי שלא למטרות עבודה עובר עברת משמעת חמורה.
2. **בעלי תפקידים**
  - ניהול ואבטחה של כלל מאגרי המידע באו"פ המכילים מידע אישי, יבוצע על-ידי בעלי התפקידים, כמפורט להלן:
    - 2.1 **מנהל מאגרי המידע** ("מנהל המאגר") – הינו האחראי ליישום מנגנוני אבטחת מידע שיבטיחו הגנה על המידע בהתאם לחוק ולצרכי האו"פ, ומהווה איש קשר מול רשם מאגרי המידע, בכל הנוגע להגדרת מאגרי המידע, תשלום אגרה שנתית, עדכונים שוטפים ועוד. ראש מינהל המחשוב הינו מנהל המאגר של האו"פ.
    - 2.2 **הממונה על אבטחת המידע** – הינו האחראי למימוש העקרונות שנקבעו במסמך מדיניות אבטחת המידע של האו"פ, תוך הפעלת שיקול דעת במציאת איזון בין דרישות האבטחה לדרישות זמינות המידע. הממונה ישולב בצמתי החלטה קריטיים בתכנון והמימוש של פיתוח מערכות מחשוב, ויהווה גורם מאשר ומבקר לפתרונות האבטחה. ראש מינהל המחשוב הינו ממונה אבטחת המידע של האו"פ.
    - 2.3 **מנהל משנה למאגר מידע** ("מנהל משנה") – הינו ראש יחידה באו"פ, האחראי על מידע בתחום מסויים, הקשור למידע אישי. מנהל המשנה ימונה על-ידי מנהל המאגר, ויהיה אחראי לפעול בהתאם לנהלי אבטחת המידע והנחיות שיופצו על-ידי מנהל המאגר וממונה האבטחה, ולקבוע בהתאמה כללי הרשאות ובקרה בכל הנוגע לשמירת הפרטיות מצד המשתמשים. פירוט מנהלי המשנה למאגרי המידע באו"פ מופיע בנספח לנוהל זה אשר יעודכן מעת לעת בהתאם למינויים.

## ניהול ואבטחת מידע אישי – 0317

2.4. **מנהל מאגר מחקר** – הינו חבר סגל אקדמי שקיבל את אישורה של ועדת האתיקה לביצוע מחקר, ומשתמש במאגר מידע בו מצוי מידע אישי, בין אם נאסף על ידו באופן עצמאי, ובין אם הגיע אליו ממאגרי המידע של האו"פ. מנהל מאגר מחקר מחויב לפעול בהתאם לנהלי אבטחת המידע והנחיות שיופצו על-ידי מנהל המאגר.

2.5. **אחראי יישום אבטחת מידע** ("אחראי יישום") – הינו האחראי ליישם כלי אבטחת מידע, להפיק הנחיות עבודה מקצועיות ולקיים תהליכי מעקב ובקרה על יישום, בהתאם לנהלים ולהנחיות ממונה האבטחה ובכפוף למסמך המדיניות. מנהל מח' טכנולוגיות ותשתיות המחשוב הינו אחראי היישום של האו"פ.

2.6. **אחראי מערכת מידע** – הגורם האחראי במינהל המחשוב או במח' שה"ם על האפיון הטכני של מערכת מידע מסויימת, על תהליכי היישום/פיתוח והבדיקות של המערכת, על ההדרכה לגבי השימוש בה ועל התפעול והתחזוקה הטכניים של המערכת.

2.7. **מומחה יישום** – הגורם האחראי ביחידה על הגדרת הדרישות והאפיון הפונקציונלי למערכת מידע מסויימת, על בדיקות הקבלה לוודוא מענה של המערכת לדרישות, על הטמעת המערכת למשתמשים ועל התפעול השוטף הנדרש של המערכת

### 3. הנחיות לאיסוף מידע אישי

מנהל משנה, אשר לצורך עבודתו נדרש לאסוף מידע אישי ולנהל אותו במאגרי המידע של האו"פ, יפעל כמפורט להלן:

3.1. יוודא כי בעת פנייה אל אדם בבקשה לקבלת מידע אישי תצורף הודעה המבהירה את המטרה שלשמה מבוקש המידע (לאילו צרכים) ומציינת למי יימסר המידע. בהמשך לפנייה, יידרש המשיב להצהיר על נכונותו למסירת המידע ולשימוש בו.

3.2. יוודא כי פרטי המידע הנאספים ומנוהלים לאורך זמן במאגר אינם חורגים מעבר למה שהוגדר ואושר לצרכים הייעודיים.

3.3. יוודא כי לאדם השייך לאוכלוסייה מסוימת (סטודנט/תלמיד/עובד) תהיה נגישות למידע אותו מסר, לצרכי צפיה או עדכון המידע, בתדירות ובאופן שיוגדרו על-ידי האו"פ וככל שמתאפשר בכפוף להרשאות ולאימות זהות.

### 4. הנחיות לגבי שימוש במידע אישי

4.1. מנהל המאגר יפיץ, מעת לעת, הנחיות בדבר מחויבותם ואחריותם של עובדים ומנהלים בארגון לנושאי ניהול ואבטחת מידע, יתן דגשים לשימוש נאות במידע אישי וימסד מנגנוני בקרה להגנה על המידע. מנהל המאגר יידע את העובדים והמנהלים לגבי קיומם של מנגנוני הבקרה.

## ניהול ואבטחת מידע אישי – 0317

- 4.2. מחלקת משו"ב תיידע כל עובד המקבל חשבון משתמש, באשר לאמור בחוק הגנת הפרטיות והנחיות בנושא אבטחת מידע, ותרענן את אותן ההנחיות אחת לשנה. בתום הרענון, העובד יחתום על טופס הצהרת משתמש, המהווה התחייבות אישית לקיום החובות החלות מכוח החוק ולמילוי הדרישות לאבטחת המידע בארגון.
- 4.3. באחריות מנהל היחידה לספק לכל עובד חדש הנחיות בעניין ניהול ואבטחת מידע אישי, הרלבנטיים למילוי תפקידו הייעודי והמוגדר ביחידה. מנהל היחידה יבצע רענון להנחיות לכלל העובדים, אחת לשנה, תוך שימת דגש מיוחד לבעלי הרשאות רחבות, כמפורט בסעיף 6.1.4 להלן.
- 4.4. בכל התקשרות של האו"פ (לרבות הזמנת רכש בתחום היעוץ) יחויב הספק/קבלן בשמירת סודיות ואבטחת מידע.

### 5. תכנון ופיתוח מערכות מידע המכילות מידע אישי

- 5.1. אחראי מערכת מידע יוודא כי היבטי אבטחת מידע אישי, הנובעים מנוהל זה ומהנחיות מנהל המאגר וממונה האבטחה, יהוו חלק בלתי נפרד משלבי הפיתוח והתפעול השוטף של המערכת, וייתחסו לכל שכבות המערכת, מרמת התשתיות והרשת ועד רמת היישום והמשתמש.
- 5.2. אחראי היישום יהיה שותף לתהליכי התכנון והמימוש של כל מערכת מידע חדשה באו"פ, וישמש כבא כוחו של מנהל המאגר וממונה האבטחה מול אחראי מערכת המידע. במסגרת תפקידו יאשר את פתרונות אבטחת המידע של המערכת, יפיק, במידת הצורך, הנחיות עבודה, ויקיים תהליכי מעקב ובקרה על אופן היישום.

### 6. בקרת שימוש ותקינות נתונים במערכות מידע המכילות מידע אישי

- 6.1. הרשאות
- 6.1.1. מנהל יחידה וכל גורם מקצועי האמון על אישור ומתן הרשאות גישה למערכות המידע, כמפורט בנוהל "חשבון משתמש והרשאה למערכות המידע", יוודא כי הרשאות הגישה של עובדים למאגר מידע המכיל מידע אישי, ייקבעו על פי הגדרת תפקיד, וינתנו בהיקף ובמידה הנדרשים לביצוע התפקיד בלבד.
- 6.1.2. מנהל יחידה יקפיד, ככל האפשר, על עקרון מידור הגישה לחלקים רגישים של מערכות המאגר, כך שלעובד יחיד לא תהיה גישה לכל החלקים הרגישים, ושביצוע פעולות חיוניות לא יהיה בשליטתו של עובד אחד בלבד.
- 6.1.3. מנהל יחידה יקפיד, ככל האפשר, על עקרון הפרדת התפקידים, כך שגורם מורשה שבסמכותו ליזום ולבצע פעולה רגישה, לא יהיה אותו גורם האמון גם על אישורה.

## ניהול ואבטחת מידע אישי – 0317

- 6.1.4. מנהל יחידה ינהל רשימה של בעלי תפקידים שהם בעלי הרשאות רחבות בגישה למידע אישי (בהתאם להיקף ההרשאות למידע ורגישות הפעולות שיכולים לבצע בו). הרשימה תועבר אחת לשנה למנהל המאגר.
- 6.2. מנהל משנה ו/או מומחה היישום יגדיר מול אחראי מערכת המידע את אמצעי הבקרה לאימות התקינות והשלמות של נתונים אישיים המוזנים על-ידי המשתמשים למערכת. ככל האפשר, יוגדרו אמצעי הבקרה לשלב בו מוזנים הנתונים למערכת. במידה ונדרש, יש להגדיר גם תהליכי בקרה תקופתיים.
- 6.3. מנהל משנה ו/או מומחה היישום יגדיר מול אחראי מערכת המידע את הפעולות שנחשבות כחריגות בשימוש במידע אישי שבמערכת, ואת תהליכי הניטור והבקרה הנדרשים לגבי פעולות אלו.
- 6.4. מנהל משנה ו/או מומחה היישום יגדיר מול אחראי מערכת המידע את משך הזמן שיישמר מידע אישי במאגר המידע (למשל, קבצי מטלות של הסטודנט). מידע שלא נדרש יותר יימחק, אלא אם הוא נדרש בהתאם לדין או לצרכי גיבוי. במקרה זה, הגיבוי יישמר בנפרד, תוך אבטחה מפני שימוש לא מורשה.
7. מסירת מידע אישי הנמצא ברשות האו"פ
- 7.1. עובד לא יוציא קובץ המכיל מידע אישי אל מחוץ לאו"פ באמצעות דואר אלקטרוני או מדיה נתיקה, אלא אם כן בוצע תהליך הצפנה למידע.
- 7.2. עובד המבקש להוציא תדפיס המכיל מידע אישי אל מחוץ לאו"פ יידע תחילה את ראש היחידה וינקוט באמצעים נאותים להגנה עליו מפני גישה של גורמים בלתי מורשים.
- 7.3. עובד שנדרש למסור קובץ המכיל מידע אישי מהאו"פ לגוף חיצוני באופן חד פעמי או קבוע, עקב התקשרות חוזית לצרכים תפעוליים של האו"פ או מכוח החוק, יעשה זאת רק לאחר קבלת אישור ממנהל המאגר והיועץ המשפטי, שיבחנו את הצורך, סבירות הבקשה ביחס לדרישות חוק הגנת הפרטיות ואמצעי הגנת המידע בגוף החיצוני. במידה והעברת המידע היא לגוף ציבורי, יש לפעול בהתאם לתקנות חוק הגנת הפרטיות.
- 7.4. מסירת מידע אישי בטלפון לסטודנט/תלמיד
- 7.4.1. לסטודנט - תתבצע רק לאחר הזדהות של הפונה באמצעות תעודת הזהות וקוד אישי. במקרים חריגים, יברר מוסר המידע את זהותו של הפונה באמצעות סדרת שאלות מתוך המידע הלימודי והדמוגרפי. לא יימסר לסטודנט מידע בטלפון לגבי ציונים, נושאי משמעת ומלגות. בקשה לשינוי פרטים אישיים (כגון, כתובת, כרטיס אשראי או מספר חשבון בנק) תתקבל בטלפון, בתנאי שהפונה הזדהה באמצעות תעודת הזהות והקוד האישי.
- 7.4.2. לתלמיד - תתבצע לאחר הזדהות של הפונה באמצעות תעודת זהות.

## ניהול ואבטחת מידע אישי – 0317

- 7.5. **מסירת מידע אישי באופן אישי לסטודנט/תלמיד** - תתבצע לאחר שהפונה שהגיע למתקני האו"פ יזדהה באמצעות תעודת זהות, דרכון תקף או רשיון נהיגה נושא תמונה.
- 7.6. **משלוח מידע אישי לסטודנט/תלמיד** - יהיה למען המופיע בפרטי הקשר (כתובת, דוא"ל, טלפון נייד) השמורים ברשותו. במאגרי המידע באו"פ.
- 7.7. **מסירת מידע אישי לקרוב משפחה של סטודנט/תלמיד**
- 7.7.1. מסירת מידע להורה של סטודנט קטין תוכל להינתן בפנייה טלפונית על ידי ציון תעודת זהות של הקטין והקוד האישי שלו, או בפניה אישית עם הצגת תעודת זהות בה מופיע שם הקטין.
- 7.7.2. מסירת מידע לבן משפחה מדרגה ראשונה של סטודנט/תלמיד תבוצע עם הצגת תעודת זהות וכן עם הצגת י"פוי כח.
- 7.7.3. מסירת מידע לכל גורם אחר תבוצע עם הצגת תעודת זהות וכן עם הצגת י"פוי כח משפטי, כדין.
- 7.8. **מסירת מידע אישי על עובדים** – עובדי משאבי אנוש יוודאו כי מידע אישי על עובד מתוך המאגר יימסר לעובד בלבד. בנסיבות המתחייבות לצרכי התפקיד, יימסר מידע אישי רלוונטי למנהליו של העובד או לבעל תפקיד אחר.

## 8. הגנה פיזית על מידע אישי

- 8.1. **הגבלת החשיפה למידע** – העובד ינקוט באמצעים סבירים למניעת גישה פיזית של גורמים בלתי מורשים למידע שעל גבי ציוד שברשותו, ובכלל זה: ישמור את שם המשתמש והסיסמאות במקום מוגן, יקפיד לצאת מיישומים פתוחים בסיום עבודה, ינעל חדר לא מאויש, יימנע מהעברת ציוד מחשוב אישי נייד בין חדרים או מהוצאתו אל מחוץ למתקני האו"פ ללא אישור אחראי הרכש במינהל המחשוב ולא ישאיר אמצעי מחשוב ניידים (לפטופ, טאבלט) במקום שחשוף לגישה לאחריים.
- 8.2. **הגנה על מסמכים חסויים**
- 8.2.1. מנהל יחידה יגדיר אמצעי הגנה פיזיים ייעודיים בהתאם לרגישות המידע במסמכים שבתחום אחריותו (למשל, תיקי עובדים), ויוודא כי לרשות העובדים המטפלים במסמכים חסויים עומדים האמצעים הנדרשים לשמירתם ואבטחתם.
- 8.2.2. העובד ינקוט באמצעים הנדרשים למניעת חשיפה של מסמך חסוי בפני גורמים בלתי מורשים, ובכלל זה: יניח מסמך שלא נדרש עוד במקומות ייעודיים לאיסוף גריסה ויאחסן מסמך הנדרש להישמר לאורך זמן במקום מוגן וממודר גישה, בתוספת הכיתוב - "מסמך חסוי".
- 8.2.3. בהגדרת תדפיס חדש ממאגר מידע המכיל מידע אישי רגיש (למשל, שכר, ציונים, מצב כלכלי/בריאותי של הסטודנט) ישלב מומחה היישום את הכיתוב "מכיל מידע מוגן".

## ניהול ואבטחת מידע אישי – 0317

- 8.2.4. עובד לא ישלח דוח המכיל מידע אישי רגיש להפקה במדפסות ציבוריות שאינן ממודרות גישה פיזית או מוגנות בקוד גישה אישי.
- 8.2.5. שליחת מסמך המכיל מידע אישי רגיש תבוצע באופן שימנע את חשיפת המידע, למעט לגורם שאליו מיועד (למשל, טופס שכר יישלח לעובד במעטפה סגורה עם הכיתוב - "אישי למכותב בלבד").
- 8.3. הגנה על אמצעי אחסון נתונים/ניידים המכילים מידע אישי – העובד ינקוט באמצעים הנדרשים למניעת חשיפה של מידע אישי המצוי באמצעי אחסון נתונים (cd, דיסק און-קי וכו') שברשותו, ובכלל זה: ישמור את אמצעי האחסון במקום מוגן וממודר גישה תוך ציון "מכיל מידע מוגן", ימחק מאמצעי האחסון מידע אישי שאינו נדרש עוד וימסור אמצעי אחסון נתיק שאינו נדרש עוד להשמדה מאובטחת (שלא תאפשר שחזור המידע).

המוסמך לאשר חריגה, במסגרת מדיניות האו"פ והוראות החוק, מהכתוב בנוהל זה: מנכ"ל האו"פ

## ניהול ואבטחת מידע אישי – 0317

### נספח – מנהלי המשנה למאגרי המידע באו"פ

מעודכן ליום 15/07/2014

מס' מאגר	שם מאגר	תיאור	מנהל משנה
990225701	משכורת - עובדי האו"פ	תשלום משכורות לעובדי האו"פ	סמנכ"ל משאבי אנוש
990028491	מערך כח-אדם	ניהול כח אדם	סמנכ"ל משאבי אנוש
980009433	הערכות עובדים	ריכוז חו"ד על עובדי המחלקות לצורך הערכה, קידום והדרכה	סמנכ"ל משאבי אנוש
990028454	קובץ הסטודנטים	רישום מידע דמוגרפי ולימודי של הסטודנט. ניהול הפעילות הכוללת של ההרשמה והלימודים	ראש מנש"ה דיקן הלימודים האקדמיים דיקן הסטודנטים מנהל ביה"ס לטכנולוגיה
990028509	תלמידי חוץ	רישום מידע דמוגרפי ולימודי של התלמידים. ניהול הפעולות הכוללות של ההרשמה והלימודים	ראש מעל"ה ראש מנש"ה
990032971	השתלמויות מורים	רישום מורים המשתתפים בקורסים, כולל מקום עבודתם והקורסים שלמדו, השכלתם וניהול הפעילות הכוללת של ההרשמה והלימודים	מנהל היחידה לקידום מקצועי של עובדי הוראה ראש מנש"ה
990035119	הנהלת חשבונות	ניהול החשבונות של האו"פ	סמנכ"ל תכנון וכלכלה
990028477	קובץ הספקים	תשלומים לספקים	סמנכ"ל תכנון וכלכלה
990029177	מאגר הידידים	ניהול פרטי קשר של החברים שהיו בעבר באגודת הידידים של האו"פ, ורישום תורמים ותרומות	מנהל יח' המשאבים

\* בחלק ממאגרי המידע יש יותר ממנהל משנה אחד, בהתאם לתחום האחריות הארגוני.

\* במאגרי המידע של האו"פ הקשורים לעובדים, משמשת חברת "חילן" כמחזיק חיצוני.