



עיריית פתח-תקוה לשכת מנכ"ל

שם הנוהל: אבטחת מידע	מספר נוהל: 30-14-007	עמוד 1 מתוך 8 עמודים
פרק: תפעול	חל על: כל יחידות העירייה	ערך: מאיר סאיג
תאריך תחולה: 06.02.2020	עדכון אחרון: 06.02.2020	מהדורה: 1

1. כללי

- 1.1 העירייה בהיותה גוף ציבורי, מחזיקה במערכות מידע ממוחשבות התומכות בפעילותה הציבורית והארגונית, כאשר במערכות אלו אגור מידע אישי וכלכלי רב.
- 1.2 מרבית המידע האישי הקיים והמעובד במערכות המידע של העירייה, הינו רגיש ומסווג כהגדרתו בחוק הגנת הפרטיות.
- 1.3 המידע, המערכות המנהלות אותו, האמצעים והציוד עליו הוא מושתת, מהווים נכס מרכזי וחיוני של העירייה ויש להגן עליהם כעל משאבים אחרים בעלי ערך בעירייה.
- 1.4 פגיעה במידע תוביל לנזקים העלולים לתת אותותיהם בהיבטים תפעוליים, טכנולוגיים וכספיים וכן להוביל לפגיעה בביטחון הפיסי, בשירותים ובצנעת הפרט של תושבים, עובדים וגורמים נוספים, שפרטיהם אגורים במערכות העירייה, וזאת מעבר לפגיעה במוניטין ובתדמית העירייה ונקיטת אמצעים משפטיים.

2. מטרה

- 2.1 להסדיר את אופן השימוש במידע רגיש, לקבוע כללים לגבי מניעת חשיפתו של המידע שלא בהסכמה, וכן לקבוע את הכללים לאבטחת המידע.
- 2.2 להבטיח את סודיות המידע הרגיש ומאגרי המידע הנאגרים במערכות המידע ומתקני העירייה.
- 2.3 להבטיח זמינות ואמינות המידע מערכות המידע לצורך המשכיות הפעילות העסקית ומתן השירות.
- 2.4 לשפר החוסן של מערכות המידע ורשתות העירייה מפני פגיעה בהיבט סודיות, אמינות וזמינות, כתוצאה מפעילות זדונית.
- 2.5 להעלות מודעות לאבטחת מידע בקרב עובדי העירייה, תוך העלאת הכשירות המקצועית של העוסקים בתחום אבטחת המידע בעירייה.

3. הפניות/מסמכים ישימים

- 3.1 חוק הגנת הפרטיות, התשמ"א - 1981.
- 3.2 תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז - 2017.
- 3.3 נספח א' - כתב התחייבות עובד לשמירת סודיות.



שם הנוהל: אבטחת מידע	מספר נוהל: 30-14-007	עמוד 2 מתוך 8 עמודים
פרק: תפעול	חל על: כל יחידות העירייה	ערך: מאיר סאיג
תאריך תחולה: 06.02.2020	עדכון אחרון: 06.02.2020	מהדורה: 1

4. הגדרות

4.1 "מידע" = כל נתון הנוגע ו/או הקשור לפעילותו, תפעולו או תפקודה של העירייה, לרבות מידע הנוגע לצנעת הפרט ומידע ציבורי רגיש, הקיים על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרוניים, על-גבי מצעי מידע פיזיים וכן מידע המועבר בעל-פה.

4.2 "אבטחת מידע" = מכלול הפעולות והאמצעים הננקטים והמיושמים בעירייה, שמטרתם להביא לכך שהמידע ופריטי הציוד היוצרים אותו והמטפלים בו, יוגנו מפני פגיעה, חשיפה, מחיקה או שינוי, במזיד או בשוגג, הן מתוך העירייה והן מחוצה לה.

4.3 "ועדת ההיגוי לנושא אבטחת מידע" = פורום ניהולי שמונה ע"י מנכ"ל העירייה ובראשו יושבים מנכ"ל העירייה או מי מטעמו ונועד לאשרר ולתקף את מדיניות העירייה בתחום אבטחת המידע, להתוות אסטרטגיות לפעילות, לפקח אחר תכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

4.4 "מנהל אבטחת המידע" = מי שמונה בכתב ע"י מנכ"ל העירייה לשמש כממונה על אבטחת המידע של העירייה ומאגריה בהתאם לסעיף 17' לחוק הגנת הפרטיות.

4.5 "עובד" = עובד עירייה, לרבות עובד השמה ועובד מיקור חוץ.

4.6 "מנהל מאגר" = גורם אשר הוסמך מטעם מנכ"ל העירייה בו הינו מועסק, לנהל מאגר מידע מסוים ואשר נרשם במשרד המשפטים כמנהלו של המאגר.

5. אחריות וסמכות

מס"ד	הגורם האחראי	תחום האחריות
1.	עובד	אחריות לשמירה על המידע המצוי בשימוש ו/או אשר הגיע לידינו/לידיעתו עפ"י נוהל זה.
2.	מנהל מאגר	- ניהול המידע במאגר ושמירה על תוכנו. - מתן הרשאות למשתמשי המאגר.
3.	מנהל אבטחת מידע	- הכוונה, פיקוח והטמעת אבטחת מידע בעירייה. - מתן הרשאות.
4.	מנהל אגף מערכות מידע	יישום הכלים והשיטות לאבטחת מידע על פי נהלים שקבעה הנהלת העירייה.



שם הנוהל : אבטחת מידע	מספר נוהל : 30-14-007	עמוד 3 מתוך 8 עמודים
פרק : תפעול	חל על : כל יחידות העירייה	ערך : מאיר סאיג
תאריך תחולה : 06.02.2020	עדכון אחרון : 06.02.2020	מהדורה : 1

6. השיטה

6.1 שמירת סודיות

- 6.1.1 כל עובד חדש הנקלט לעבודה בעירייה יחתום על כתב התחייבות עובד לשמירה סודיות (ראה נספח א').
- 6.1.2 חל איסור לשתף גורם שאינו מורשה במידע סודי הקשור לעבודה בעיריית פתח-תקוה, בדגש על פרטים אישיים ועסקיים של ספקים ותושבים.
- 6.1.3 העובד מתחייב שלא למסור כל מידע, רגיל וממוחשב, שהגיע אליו בתוקף תפקידו, לכל גורם, אלא אם כן הורשה לכך או שהדבר נעשה במסגרת תפקידו.
- 6.1.4 על העובד לשמור על סודיות המידע והנתונים אליהם הוא נחשף במהלך עבודתו.
- 6.1.5 הוראה זו חלה על העובד גם לאחר שסיים את עבודתו בעירייה.
- 6.1.6 יש לגרוס כל נייר המכיל מידע רגיש, כאשר אין בו עוד צורך.

6.2 סיסמאות

- 6.2.1 שם המשתמש והסיסמא הם אישיים, ונועדו אך ורק לשימוש האישי של העובד ולצורך ביצוע עבודתו.
- 6.2.2 חל איסור למסור את שם המשתמש והסיסמא האישיים לאדם אחר או להשתמש בשם משתמש וסיסמא של עובד אחר במהלך העבודה.
- 6.2.3 יש להימנע משמירת הסיסמא במקום בו היא עלולה להיחשף (תיקיות ציבוריות, הדבקת פתק באזור העבודה וכו').
- 6.2.4 בכל מקרה של חשיפת הסיסמא או חשד לחשיפתה, יש להחליף את הסיסמא מיידית ולדווח למנהל אבטחת המידע על המקרה.

6.3 אבטחת סביבת העבודה

- 6.3.1 כל עובד/ת אחראי/ת לאבטחת סביבת העבודה האישית שלו. אבטחת סביבת העבודה תתבסס על שני עקרונות מרכזיים :
- 6.3.2 **מדיניות "שולחן נקי" (Clear desk policy) :**
- א. מסמכים רגישים לא יותרו חשופים על השולחן כאשר העובד עוזב את סביבת העבודה בסוף או במהלך יום העבודה.
- ב. בעת עזיבת סביבת העבודה ינעל העובד את המסמכים הרגישים בארון נעול.



עיריית פתח-תקוה לשכת מנכ"ל

שם הנוהל: אבטחת מידע	מספר נוהל: 30-14-007	עמוד 4 מתוך 8 עמודים
פרק: תפעול	חל על: כל יחידות העירייה	ערך: מאיר סאיג
תאריך תחולה: 06.02.2020	עדכון אחרון: 06.02.2020	מהדורה: 1

ג. ניירת רגישה תושם בפח ייעודי אשר תכולתו מיועדת לגריסה. יש לגרוס כל ניירת משרדית, שאין בה עוד צורך ובפרט ניירת המכילה מידע "סודי".
ד. במידה ולא קיים פח מעין זה בסביבת העבודה של המשתמשים באחריות המשתמש לגרוס את הניירת.

6.3.3 מדיניות "מסך נקי" (Clear screen policy):

א. אין להותיר את המחשב פתוח (במצב של חיבור לרשת), כאשר עוזבים את סביבת העבודה. על העובד לצאת באופן מסודר מהרשת (log off) ולכבות את המחשב.
ב. בכל מקרה של "נטישת" עמדת המחשב, יפעיל המשתמש את שומר המסך באופן ייזום באמצעות לחיצה על המקשים **Alt+Ctrl+Delete**.
ג. מידע תפעולי של העירייה ישמר בכונן הרשת בלבד ולא על עמדות מחשב. הגישה למידע תתאפשר בהתאם לרמת ההרשאות שניתנה לעובד ובהתאם לעקרון "הצורך לדעת".

6.4 תוכנות

6.4.1 עיריית פתח תקווה מייחסת חשיבות רבה להתקנת תוכנות חוקיות בלבד על כל המחשבים בעירייה, ולכן חל איסור שימוש בתוכנות בלתי חוקיות.
6.4.2 חל איסור מוחלט להתקין במחשבי העירייה תוכנות ללא אישור בכתב מאגף מערכות מידע.

6.5 מחשבים ניידים (לפטופ)

6.5.1 המחשב הינו אישי ולשימושו של העובד בלבד.
6.5.2 חל איסור לבצע תחזוקה של המחשב הנייד ע"י גורם מחוץ לעירייה.
6.5.3 כאשר העובד מנייד את המחשב (הנייד או הנייח) מחוץ לעירייה, המחשב יהיה תמיד תחת השגחתו.
6.5.4 אם הלפטופ אבד או נגנב, יש לדווח מיידית לאגף מערכות מידע.

6.6 שימוש נאות בציוד העירייה

6.6.1 יש להימנע משימוש לצרכים פרטיים בציוד המחשוב של העירייה.
6.6.2 חל איסור להפסיק את פעולת המערכות לאבטחת מידע, כגון אנטי וירוס.
6.6.3 חל איסור לשנות את הגדרות המערכת של המחשב.
6.6.4 אין להפיץ תכנים נושאי אופי מיני או מידע אחר העלול להוות עלבון ליחיד או לקבוצה או כל חומר המפר את הנחיות העירייה בנושא הטרדה מינית.
6.6.5 חל איסור על התקנה, הורדה או אחסון של מידע המוגן בזכויות יוצרים.



שם הנוהל : אבטחת מידע	מספר נוהל : 30-14-007	עמוד 5 מתוך 8 עמודים
פרק : תפעול	חל על : כל יחידות העירייה	ערך : מאיר סאיג
תאריך תחולה : 06.02.2020	עדכון אחרון : 06.02.2020	מהדורה : 1

6.7 ניהול מצעים ניידים

- 6.7.1 חל איסור מוחלט לחבר במחשבי העירייה או לרשת הארגונית רכיבי ציוד תוכנה וחומרה באביזרים נלווים כגון דיסקים ניידים Disk on key, טלפונים ניידים וכדומה ללא אישור של מנכ"ל העירייה או מנהל מערכות המידע או סגנו או מנהל אבטחת מידע.
- 6.7.2 חל איסור להוציא מידע על כל מצע, ממשקי USB, דיסקים ניידים, Disk on key ונתיקים, וכ"ל ללא אישור מראש ובכתב של מנהלי היחידות.
- 6.7.3 כאשר שומרים מידע חסוי על גבי מדיה נתיקה, יש לאחסן אותו על גבי Disk on key מוצפן אשר יסופק ע"י העירייה בלבד ולא במדיה אחרת.
- 6.7.4 ניירת או מצע מידע אחר (דיסקים, Disk On Key), יאוחסנו במקום מאובטח כגון מגירות או ארונות נעולים.

6.8 העברת מידע ואבטחת פלטי מחשב

- 6.8.1 חל איסור להוציא מידע מהעירייה, למעט במקרים שאושרו ע"י המנהל הישיר ולפי צרכי העבודה.
- 6.8.2 מסירת מידע לגופים ואנשים מחוץ לעירייה, ייעשה בכפוף לכל דין.
- 6.8.3 עובד שהוסמך לקבל דו"ח מחשב מסווג, ישתמש בדו"ח לצורכי העבודה ולא ימסור אותו לעובד אחר, אלא אם כן אישר זאת מנהל היחידה.
- 6.8.4 מידע המכיל ריכוז פרטים לגבי אנשים ומסווג כמידע רגיש עפ"י הוראות חוק הגנת הפרטיות וכן כל מידע אחר של העירייה, יימצא תחת משמורת המחזיק בו בכל זמן נתון.
- 6.8.5 משלוח רשומות נייר רגישות בדואר רגיל ודואר אלקטרוני שסיווגם "חסוי"/"סודי", יועברו בשיטות ובאמצעים המקובלים בעירייה.

6.9 שימוש באינטרנט

- 6.9.1 חל איסור לשתף מידע של העירייה באמצעות היישומים השונים באינטרנט.
- 6.9.2 יש להימנע ממסירת פרטים אישיים של העובד, וחל איסור למסור את כתובת הדואר האלקטרוני של העירייה בעת רישום לאתרי אינטרנט, למעט רישום לאתרים הקשורים לעבודתו של העובד.
- 6.9.3 חל איסור לגלוש באתרים בעלי תוכן פוגעני.



עיריית פתח-תקוה לשכת מנכ"ל

שם הנוהל : אבטחת מידע	מספר נוהל : 30-14-007	עמוד 6 מתוך 8 עמודים
פרק : תפעול	חל על : כל יחידות העירייה	ערך : מאיר סאיג
תאריך תחולה : 06.02.2020	עדכון אחרון : 06.02.2020	מהדורה : 1

6.10 שימוש בדואר אלקטרוני

6.10.1 תיבת הדואר האלקטרונית בעירייה הינה תיבה מעורבת, ויחד עם זאת יש להמעיט השימוש בה לצרכים אישיים.

6.10.2 חל איסור על המעביד או על כל עובד אחר להיכנס לתיבת הדוא"ל ולכל

אמצעי אחר המכיל מידע פרטי של עובד ללא אישור של העובד בכתב.

6.10.3 חל איסור לשלוח מכתבי שרשרת, מיילים והודעות בעלי תוכן פוגעני או כאלה, אשר עלולים לפגוע במהלך התקין של העבודה או בתדמיתה של העירייה.

6.10.4 אין לפתוח הודעות דואר אלקטרוני או קבצים מצורפים אשר מקורם אינו מוכר או אינו סביר.

6.10.5 עובד שקיבל מייל חשוד בתיבת המייל שסופקה לו לצורך עבודתו, ידווח במיידית לאגף מערכות המידע.

6.11 רשתות חברתיות

6.11.1 בזמן שימוש ברשתות חברתיות, חלים כל הכללים בנוהלי העירייה, בקשר להוצאת מידע ושמירת סודיות. אין לפרסם תכנים של העירייה המוגדרים בחיסיון מטעמי אבטחת מידע או הגנת הפרטיות.

6.11.2 אם עובד בעירייה בחר לציין את עובדת היותו עובד בעירייה, מחובתו להבהיר שדבריו נאמרים על דעת עצמו ולא מטעם העירייה.

6.12 דיווח על אירועי אבטחת מידע

6.12.1 חלה חובה על המשתמש לדווח על אירועים/בעיות אבטחת מידע בהם הוא נתקל במהלך עבודתו ובהם :

א. חשד לפרצות אבטחת מידע במערכות השונות ובמחשב האישי.

ב. חשד כלשהו כי המידע האגור במערכות נפגע (נמחק, שונה או נחשף).

ג. חשד לקבלת מייל דייג (fishing).

ד. חשד של המשתמש כי נעשה שימוש לא מורשה בזיהוי המשתמש שלו.

6.12.2 הדיווח יעשה במייל למרכז התמיכה עם העתק למנהל אבטחת המידע. יש לצרף את מירב הפרטים ככל שניתן.



שם הנוהל : אבטחת מידע	מספר נוהל : 30-14-007	עמוד 7 מתוך 8 עמודים
פרק : תפעול	חל על : כל יחידות העירייה	ערך : מאיר סאיג
תאריך תחולה : 06.02.2020	עדכון אחרון : 06.02.2020	מהדורה : 1

7. חתימות

כתבו :

אליהם כהן	ז' בחשוון תש"ף – 05.11.2019
מנהל אבטחת מידע	תאריך

מאיר סאיג	ז' בחשוון תש"ף – 05.11.2019
הממונה על הנהלים	תאריך

אישרו :

ענת שלומוביץ	כו' בחשוון תש"ף – 24.11.2019
מנהלת אגף מערכות מידע	תאריך

אלי שלמה	כח' בחשוון תש"ף – 26.11.2019
יו"ר ארגון העובדים	תאריך

עו"ד שרית גרינבאום	יז' בטבת תש"ף – 14.01.2020
יועצת משפטית לעירייה	תאריך

יניב בניטה	כג' בטבת תש"ף – 20.01.2020
מנכ"ל העירייה	תאריך

רמי גרינברג	כד' בטבת תש"ף – 21.01.2020
ראש העיר	תאריך



שם הנוהל: אבטחת מידע	מספר נוהל: 30-14-007	עמוד 8 מתוך 8 עמודים
פרק: תפעול	חל על: כל יחידות העירייה	ערך: מאיר סאיג
תאריך תחולה: 06.02.2020	עדכון אחרון: 06.02.2020	מהדורה: 1

נספח א'

כתב התחייבות עובד לשמירת סודיות

אני הח"מ _____ ת"ז _____ מאשר/ת שקראתי את נוהל אבטחת המידע של עיריית פתח-תקוה, והנני מצהיר ומתחייב כלפי העירייה כדלקמן:

הנני מתחייב לשמור בסודיות ולא לגלות ו/או למסור ו/או להעתיק לשום אדם ו/או גוף או לחילופין עבור שום אדם ו/או גוף, ידיעות ו/או מידע ו/או מסמכים כלשהם שהגיעו ו/או שיגיעו לידי במסגרת עבודתי בעירייה בין במישרין ובין בעקיפין, ולא אעשה כל שימוש בידיעות, מידע ומסמכים כאמור, במסגרת תפקידי ו/או לאחר סיום תפקידי.

הריני מתחייב לנקוט בכל אמצעי הזהירות, כדי למנוע אפשרות שיצא מרשותי מידע ויגיע לידי מי שלא הוסמך לקבלו. כמו כן, אני מתחייב כי אם אקבל רשות להשתמש במאגרי המידע של העירייה, אעשה זאת אך ורק לצורך מתן השירותים בעירייה.

הריני מתחייב כי לאחר סיום עבודתי בעירייה, מכל סיבה שהיא, לא אשאיר ברשותי כל מסמך ו/או חומר שנמסרו לי או הגיעו לרשותי בעקבות ו/או כתוצאה מעבודתי בעירייה ולהחזיר מיד, כל מידע כאמור עם סיום עבודתי בעירייה ו/או להשמיד בתיאום מראש עם העירייה כל מידע שנאסף ו/או נשאר ברשותי ושלא הועבר לרשות העירייה.

התחייבות זו לא תחול כל אימת שהוסמכתי במפורש ע"י הממונים עליי לנהוג אחרת, וכן לא תחול כלפי מי, שהדין מחייב כלפיו בגילוי או כל אימת שהדבר נועד למסירת מידע במסגרת חילופי מידע מקצועיים.

ידוע לי כי היה ואפר התחייבות זו העירייה עלולה לפעול נגדי בכל האמצעים העומדים לרשותה על פי הדין.

התחייבותי זו איננה מוגבלת בזמן, והיא תוסיף לחול אף לאחר תום תקופת עבודתי בעירייה.

ולראיה באתי על החתום

תאריך: _____ חתימה: _____