	שם הנוהל: **נוהל הנחיות אבטחת מידע לעובד בארגון**	סיווג המסמך: **חסוי** 1/5
	שם מחלקה: אבטחת מידע	תאריך פרסום:
	מספר הנוהל: **3**	גרסה: **1.0**

אל מחלקת משאבי אנוש

<u>הנדון: הנחיות אבטחת המידע לעובד "רשות מועצה אזורית אשכול"</u>

הנני מאשר כי קראתי את ההוראות וההנחיות בנוגע להנחיות אבטחת מידע כאמור לעיל בנוהל זה וכי הבנתי את תוכנן ומשמעותן ואת חובותיי על פיהן.
ידוע לי כי במידה ולא אמלא את חובותיי כאמור לעיל, עלולים להינקט כנגדי צעדים וסנקציות בהתאם לחוק ולנהלי המשרד.

שם העובד: _____ **תפקיד:** _____

תאריך: _____ **חתימה:** _____

נוהל הנחיות אבטחת מידע לעובד בארגון

- מסמך זה מותר לשימוש פנימי בלבד.
- כל האמור בנוהל זה בלשון זכר או להיפך נעשה מטעמי נוחות ויש לראותו כאילו נאמר גם בלשון נקבה או להיפך.
- בדוק שהנך עושה שימוש בגרסה האחרונה של המסמך!
- בכל מקרה בו נדרש לערוך שינויים בנוהל זה, יש לפנות אל אחראי הנהלים "רשות מועצה אזורית אשכול"

נתונים כללים

ערך: מתן שטרית	
בדק:	
אישר:	
סוג המסמך: מדיניות ונהלים	
תאריך פרסום המסמך: 01.02.2019	תאריך תיקוף המסמך:
סטאטוס המסמך: סופי	

טבלת שינויים

תאריך שינוי	מהות השינוי	סעיפי השינוי	גרסה	גורם מאשר

	שם הנוהל: **נוהל הנחיות אבטחת מידע לעובד בארגון**	סיווג המסמך: **חסוי** 3/5
	שם מחלקה: אבטחת מידע	תאריך פרסום:
	מספר הנוהל: **3**	גרסה: **1.0**

1. כללי:;

1.1. עובדי **"רשות מועצה אזורית אשכול"** (להלן "**הארגון**") עלולים להיחשף במהלך ביצוע תפקידם למידע חסוי.

1.2. כל מידע חסוי אליו תחשפו במהלך עבודתכם בארגון, מחויב להיות מוגן עפ"י:

1.2.1. חוק הגנת הפרטיות (1981).

2. שמירת סודיות

2.1. חל איסור לשתף גורם שאינו מורשה במידע חסוי הקשור לעבודה בארגון (כולל שיתוף עמיתים לעבודה אשר המידע אינו רלוונטי לעבודתם).

2.2. על העובדים להקפיד לשמור על סודיות המידע גם בנושאים והתהליכים הבאים:

2.2.1. מסכי מחשב המכילים מידע חסוי ואת שמו של הלקוח יוצבו כך שהמידע לא ייחשף לגורמים לא מורשים.

2.2.2. הקפדה כי גורמים לא מורשים אינם נחשפים למידע חסוי במהלך שיחות בין צוות הארגון, ובמהלך מסירת מידע פרונטאלי ללקוח עצמו.

2.2.3. יש לגרוס כל מסמך או נייר המכיל מידע אישי חסוי.

2.3. תוקפו של ההסכם באשר למידע עסקי – 7 שנים תום ההעסקה.

2.4. חובת שמירת הסודיות חלה גם לאחר סיום ההעסקה בארגון.

3. הוצאת מידע מהארגון

3.1. חל איסור חמור להוציא מידע חסוי מהארגון למעט במקרים שאושרו ע"י המנהל הישיר וצרכי העבודה מחייבים זאת.

3.2. אין להוציא מצעי מידע המכילים מידע חסוי אל מחוץ לכותלי הארגון, אלא באישור מיוחד של מנהל תחום אבטחת המידע והמנהל הישיר. כמו כן אין להעביר מידע לגורמים חיצוניים אלא באישור מנהל תחום אבטחת מידע והמנהל הישיר.

4. קבלת קהל

4.1. במחלקות בהן יש קבלת קהל עולה הסיכון לאבטחת המידע בארגון, מכיוון שגורמים לא מוכרים מקבלים גישה למחלקות בארגון.

4.2. בזמן קבלת קהל על עובדי הארגון להגביר את הערנו בנוגע לאבטחת המידע החסוי.

5. התקנת תוכנות

5.1. חל איסור מוחלט להתקין במחשבי הארגון תוכנות. כל תוכנה תותקן על המחשב ע"י מנהל המחשוב בלבד ולאחר שאושרה בהיבטי מחשוב ואבטחת מידע. לא יאושרו תוכנות העלולות לפגוע בתפקוד המחשב, תפקוד רשת הארגון או לחשוף מידע חסוי.

5.2. חל איסור מוחלט לעשות שימוש בתוכנות לא חוקיות.

5.3. בכל מקרה של צורך בתוכנה חדשה, יש לפנות למנהל המחשוב ולבצע את הרכישה וההתקנה באמצעותו.

	שם הנוהל: **נוהל הנחיות אבטחת מידע לעובד בארגון**	סיווג המסמך: **חסוי** 4/5
	שם מחלקה: אבטחת מידע	תאריך פרסום:
	מספר הנוהל: **3**	גרסה: **1.0**

6. שם משתמש וסיסמא

6.1. שם המשתמש הוא אישי ונועד לשימושו של המשתמש בלבד ולצורך ביצוע עבודתו.

6.2. חל איסור למסור את שם המשתמש והסיסמא שלך לאדם אחר או להשתמש בשם משתמש וסיסמא של עובד אחר במהלך עבודתך.

6.3. הסיסמא מהווה מפתח גישה למידע רגיש ביותר ולמערכות, ולפיכך עליה להיות אישית וסודית. עבודה על מערכות המחשוב בארגון תחת שם משתמש של עובד אחר.

6.4. יש להימנע משמירת הסיסמא במקום בו היא עלולה להיחשף.

6.5. בכל מקרה של חשיפת הסיסמא או חשד לחשיפתה, יש להחליף את הסיסמא מיידית ולדווח למנהל תחום אבטחת המידע על המקרה.

7. עמדת עבודה

7.1. חל איסור חמור לשמור מידע חסוי על גבי המחשב המקומי.

7.2. עובד העוזב את עמדתו ינעל את מחשבו (ע"י פקודת CTRL+ALT+DEL).

7.3. בתום יום העבודה יבוצע תהליך סיום עבודה מסודר הכולל יציאה מכל המערכות וכיבוי של תחנת העבודה.

7.4. יש להקפיד על קיום מדיניות "שולחן נקי", הכוללת ניקוי שולחן העבודה מכל ניירת או מדיה המכילים מידע בסיווג "חסוי", "חסוי ביותר".

7.5. יש להקפיד לאחסן כל נייר או מדיה המכילים מידע "חסוי" או "חסוי ביותר" במיקום מאובטח (ארון נעול, מגירה נעולה או כספת) בתום יום העבודה או בעת עזיבת העמדה.

7.6. יש לוודא כי לגורמים שאינם מוסמכים (עמיתים לעבודה, אורחים, ספקים, קהל), לא תהיה גישה לחומרים המכילים חומרים בסיווג חסוי או חסוי ביותר.

7.7. יש לגרוס כל נייר משרדי שאין בו עוד צורך ובפרט נייר המכיל מידע חסוי ו\או מידע חסוי ביותר.

8. שימוש באינטרנט

8.1. חל איסור להעביר מידע שהינו חסוי וחסוי ביותר באמצעות היישומים השונים שברשת האינטרנט, אלא עפ"י הנחיות מנהל תחום אבטחת המידע במשרד.

8.2. אין לבצע הורדת קבצים מרשת האינטרנט. אישור חריג להורדת קבצים, יינתן רק לפי צורך הכרחי וחיוני, ובפניה למנהל המחשוב.

8.3. יש להימנע ממסירת פרטים אישיים של העובד וחל איסור למסור את כתובת הדואר האלקטרוני של הארגון בעת רישום לאתרי אינטרנט, למעט רישום לאתרים הקשורים לעבודתו של העובד.

9. שימוש נאות בציוד הארגון

9.1. חל איסור לבצע בציוד המחשוב של הארגון כל פעילות החורגת ממסגרת התפקיד.

9.2. חל איסור לבצע שימוש פרטי בציוד המחשוב של הארגון.

9.3. חל איסור לחבר או להכניס מדיה מגנטית פרטית או של גורם חיצוני למחשבי הארגון (דיסק און קיי, CD, DVD, דיסק קשיח חיצוני, וכו').

9.4. חל איסור לחבר טלפונים סלולריים למחשבי הארגון.

9.5. חל איסור להפסיק את פעולת המערכות לאבטחת מידע, כגון אנטי וירוס.

9.6. חל איסור לשנות את הקונפיגורציה של המחשב.

10. שימוש בדואר אלקטרוני

10.1. השימוש בדואר אלקטרוני נועד לצורכי העבודה והתפקיד ולא לצרכים פרטיים.

10.2. חל איסור לשלוח מיילים בעלי תוכן פוגעני.

10.3. חל איסור לשלוח מכתבי שרשרת ושאר מיילים המפריעים למהלך התקין של העבודה.

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

11. שימוש במדפסות ובמכשירי פקס

11.1. העובד אחראי לאסוף את החומר מהמדפסת מיד לאחר שליחתו להדפסה, על מנת לוודא כי החומר המודפס לא יילקח ע"י גורם לא מורשה.

11.2. העברת מידע בפקס: יש להפעיל שיקול דעת לפני העברת מידע בפקס תוך התייחסות לסיכונים הכרוכים בכך.

11.3. במקרה של מכשיר פקס מרכזי, הנמצא בשטח ציבורי, יש להשגיח שהחומר הנכנס או היוצא לא יילקח ע"י אדם אחר.

12. אבטחה פיזית

12.1. במחלקות ואזורים בארגון שאסורים לכניסת מבקרים או מחוץ לשעות הביקור, יש להקפיד כי גורמים שאינם מורשים או אינם מוכרים לא יכנסו אל שטחי אתרי הארגון בעת כניסתך או צאתך מהמחלקות והשטחים השונים.

12.2. יש לנעול את דלת המשרד בסוף יום העבודה.

12.3. בכל מקרה בו מזהה העובד גורמים שאינם מוכרים לו או מתנהלים בצורה חשודה במחלקות ובאזורי העבודה השונים, יש לוודא את זהות הגורם וללוות לנקודה אליה צריך להגיע. בכל חשד לפעילות לא חוקית, יש לדווח מידית למנהל הישיר ולאיש הביטחון.

13. דיווח על אירועי אבטחת מידע

13.1. עובד המזהה אירוע \ בעיית אבטחת מידע ידווח עליו באופן מידי למנהל תחום אבטחת המידע בארגון.

13.2. סוגי אירועי אבטחה עליהם יש לדווח, יכללו בין היתר:

- עבירות אבטחת מידע הנעשות ע"י העובד\ת עצמו\ה ו\או עובדים אחרים.
- חשד לפריצות אבטחת מידע במערכות השונות ובמחשב האישי.
- חשד כלשהו כי המידע האגור במערכות נפגע (נמחק \ שונה \ נחשף).
- חשד של עובד\ת כי נעשה שימוש לא מורשה בזיהוי המשתמש שלו.