



נוהל, הצהרה והנחיות אבטחת מידע לעובד

1. כללי

- 1.1 כל עובד יהיה אחראי באופן אישי לאבטחת המידע אליו הוא נחשף במהלך עבודתו. כל פגיעה במידע הנובעת מרשלנות העובד תהיה באחריות העובד ועלולה לגרור הפעלת אמצעי משמעת כנגדו.
- 1.2 כל פגיעה במידע אשר בוצעה ע"י העובד במזיד תגרור הפעלת אמצעי משמעת כנגדו.
- 1.3 נהלי אבטחת מידע של המועצה להסדר ההימורים בספורט מפורסמים בספריה [PUBLIC](#)
- 1.4 כל עובד מחויב לקרוא את נהלי אבטחת מידע, להכירם ולנהוג על פיהם.

2 עיקרון האחריות האישית

כל עובד המועצה להסדר ההימורים בספורט אחראי באופן אישי לאבטחת המידע אליו הוא נחשף במהלך עבודתו. על העובד לנקוט בכל האמצעים העומדים לרשותו על מנת להגן על מידע זה.

3 שמירת סודיות

- 3.1 כל עובדי המועצה להסדר ההימורים בספורט מחויבים לשמור על סודיות המידע והנתונים אליהם הם נחשפים במהלך עבודתם.

4 התקנת תוכנות

- 4.1 חל איסור מוחלט להתקין במחשבי החברה תוכנות ללא אישור בכתב של מנהל ה-IT. כל תוכנה תאושר בהיבטי מחשוב ואבטחת מידע. לא יאושרו תוכנות העלולות לפגוע בתפקוד המחשב, תפקוד רשת או לחשוף מידע.
- 4.2 בכל מקרה של צורך בתוכנה חדשה, יש לפנות לצוות ה-IT ולבצע את הרכישה וההתקנה באמצעותה.

5 שם משתמש וסיסמא

- 5.1 שם המשתמש הוא אישי ונועד לשימוש של המשתמש בלבד ולצורך ביצוע עבודתו.
- 5.2 הסיסמא מהווה מפתח גישה למידע רגיש ביותר ולמערכות, ולפיכך עליה להיות אישית וסודית.
- 5.3 חל איסור למסור את שם המשתמש והסיסמא שלך לאדם אחר או להשתמש בשם משתמש וסיסמא של עובד אחר במהלך עבודתך.
- 5.4 חל איסור על שמירת הסיסמא במקום בו היא עלולה להיחשף.



5.5 בכל מקרה של חשיפת הסיסמא או חשד לחשיפתה, יש להחליף את הסיסמא מידית ולדווח לממונה על אבטחת המידע על המקרה.

6 עזיבת עמדת העבודה

- 6.1 משתמש העוזב את עמדתו ינעל את מחשבו (CTRL+Alt+Delete).
- 6.2 בתום יום העבודה יבוצע תהליך סיום עבודה מסודר הכולל יציאה מכל המערכות וכיבוי של תחנת העבודה.
- 6.3 יש להקפיד על קיום מדיניות "שולחן נקי", הכוללת ניקוי שולחן העבודה מכל ניירת או מדיה בסיווג רגיש.
- 6.4 יש להקפיד לאחסן כל נייר או מדיה המכילים מידע "רגיש" במיקום מאובטח (ארון נעול, מגירה נעולה או כספת) בתום יום העבודה או בעת עזיבת העמדה.
- 6.5 יש לוודא כי לגורמים שאינם מוסמכים (עמיתים לעבודה, אורחים, ספקים, קהל), לא תהיה גישה לחומרים בסיווג רגיש.
- 6.6 יש לגרוס כל נייר משרדי שאין בו עוד צורך.

7 שימוש באינטרנט

- 7.1 אין לבצע הורדת קבצים מרשת האינטרנט. אישור חריג להורדת קבצים, יינתן רק לפי צורך הכרחי וחיוני, ובפניה לממונה אבטחת מידע.

8 שימוש נאות בציוד המשרד

- 8.1 חל איסור לחבר או להכניס מדיה מגנטית פרטית או של גורם חיצוני למחשבי החברה
- 8.2 חל איסור לחבר טלפונים סלולריים למחשבי החברה.
- 8.3 חל איסור להפסיק את פעולת המערכות לאבטחת מידע כגון אנטי וירוס.
- 8.4 חל איסור לשמור מסמכים של המועצה להסדר ההימורים בספורט על הדיסק המקומי של המחשב הנייח. מסמכים אלו ישמרו על כונן X.
- 8.5 תותקן תוכנת אנטי וירוס על מחשבים ניידים.
- 8.6 חל איסור לשנות את קונפיגורציית המחשב.

9 שימוש בדואר אלקטרוני

- 9.1 השימוש בדואר אלקטרוני נועד לצורכי העבודה והתפקיד ולא לצרכים פרטיים.
- 9.2 חל איסור לשלוח מיילים בעלי תוכן פוגעני.
- 9.3 חל איסור לשלוח מכתבי שרשרת ושאר מיילים המפריעים למהלך התקין של העבודה.
- 9.4 אין לפתוח הודעות דואר אלקטרוני או קבצים מצורפים אשר מקורם אינו מוכר או אינו סביר.



10 שימוש במדפסות

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

11 אבטחה פיזית

11.1 יש להקפיד כי גורמים שאינם מורשים או אינם מוכרים לא יסתובבו האופן חופשי ללא השגחה במשרדים.

11.2 בכל מקרה בו מזהה העובד גורמים שאינם מוכרים לו או מתנהלים בצורה חשודה באזורי העבודה השונים, יש לוודא את זהות הגורם וללוותו לנקודה אליה צריך להגיע. בכל חשד לפעילות לא חוקית, יש לדווח מיידית לממונה אבטחת המידע.

12 עבודה עם מחשב נייד

12.1 יש להימנע לחלוטין משמירת מידע בסיווג רגיש על המחשב הנייד.

12.2 מידע יישמר אך ורק ברשת של המועצה להסדר ההימורים בספורט.

12.3 כאשר משתמשים במחשב נייד במקומות ציבוריים, בחדרי ישיבות ובאזורים מחוץ לחצרי המועצה, יש להיזהר במיוחד ולמנוע גישה וחשיפה לא מורשית למידע המאוחסן והמעובד במחשבים.

12.4 יש להקפיד על קיום תכנת אנטי וירוס מעודכנת וכן כל תכנה אחרת המקובלת בארגון גם על גבי המחשבים הניידים. יש להתחבר לרשת המועצה לפחות אחת לחודש על מנת לעדכן את המחשב בחבילות התכנה וחתימות האנטי וירוס העדכניות.

12.5 אין להשאיר את המחשב הנייד ברכב.

13 דיווח על אירועי אבטחת מידע

עובד המזהה אירוע / בעיית אבטחת מידע ידווח עליו באופן מיידי לממונה אבטחת מידע .
סוגי אירועים עליהם יש לדווח:

13.1 עבירות אבטחת מידע הנעשות ע"י העובד/ת עצמו/ה ו/או עובדים אחרים

13.2 חשד לפריצות אבטחת מידע במערכות השונות ובמחשב האישי

13.3 חשד כלשהו כי המידע האגור במערכות נפגע (נמחק/ שונה /נחשף)

13.4 חשד של עובד/ת כי נעשה שימוש לא מורשה בזיהוי המשתמש שלו.

**אני מצהיר כי קראתי את ההוראות וההנחיות בנוגע להנחיות אבטחת מידע כאמור לעיל
בנוהל זה וכי הבנתי את תוכנו ומשמעותו ואת חובותיי על פיהן .**



נהלי אבטחת מידע

ידוע לי כי במידה ולא אמלא את חובותיי כאמור לעיל, עלולים להינקט כנגדי צעדים
וסנקציות בהתאם לחוק ולנהלי החברה.

שם העובד: _____ תפקיד: _____

תאריך: _____ חתימה: _____