נספח ב': הנחיות אבטחת מידע לחבר קהילת וולקני

נוהל, הצהרה והנחיות אבטחת מידע לחבר קהילת וולקני

1. <u>כללי</u>

1.1. <u>קהילת וולקני-</u> כל עובדי המכון, מלגאים, פוסט דוקטורנטים, מתנדבי שירות לאומי ,עובדי מיקור חוץ וכל מי שמבצע את משימותיו באופן קבוע וסדיר במכון.

1.2. <u>מידע חסוי</u> - כל מידע אשר גילויו לגורמים בלתי מוסמכים עשוי לגרום נזק בינוני או כבד למכון. מידע שחשיפתו לגורמים מחוץ למכון עלול לגרום נזק למטרותיהם, יעדיהם, שמם הטוב, אמינותם או נזק כלכלי פיננסי למכון או לעובדיו. (לדוגמא: תרשים הנדסי של המבנים , תרשים של רשת המחשבים והגדרותיה, הסכמים עם גורמי חוץ)

2. <u>**עיקרון האחריות האישית**</u>

2.1. כל חבר קהילת וולקני אחראי באופן אישי לאבטחת המידע אליו הוא נחשף במהלך עבודתו. על החבר קהילה לנקוט בכל האמצעים העומדים לרשותו על מנת להגן על מידע זה.

3. <u>שמירת **סודיות**</u>

3.1. כל חבר קהילת וולקני מחויבים לשמור על סודיות המידע והנתונים אליהם הם נחשפים במהלך עבודתם.

3.2. חל איסור לשתף גורם שאינו מורשה במידע חסוי הקשור לעבודה במכון.

4. <u>מסירת מידע **חסוי**</u>

4.1. ככלל חל איסור להוציא ו/או למסור מידע חסוי מחוץ למכון.

4.2. במידה ונדרשת העברת מידע חסוי , ביצוע העברת המידע יאושר ע"י המנהל הישיר ובהתאם להנחיה ד של מנהל המכון ,

5. <u>הוצאת מידע מהמכון</u>

5.1. חל איסור חמור להוציא מידע/מצעי מידע חסוי מהמכון למעט במקרים הנדרשים ושאושרו ע"י המנהל הישיר וצרכי העבודה מחייבים זאת.

5.2. בכל מקרה של הוצאת מידע ינקטו כל האמצעים הנדרשים לאבטח את המידע מחוץ למשרד. (לדוגמה אין להשאיר את המחשב ללא השגחה גם לא בכלי הרכב)

6. <u>חיבור ציוד לרשת המכון</u>

6.1. חל איסור לחבר לרשת המכון ציוד שלא אושר ע"י אגף המחשוב .

6.2. במידה ויש צורך לחבר ציוד הנדרש לביצוע עבודה, צריך לקבל אישור ממונה אבטחת המידע .

7. <u>התקנת תוכנות</u>

7.1. המכון רוכש תוכנות הנדרשות לצורך העבודה, אין להוריד תוכנות באופן לא חוקי ולהתקינן על המחשב.

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

7.3. הסיסמא מהווה מפתח גישה למידע רגיש ביותר ולמערכות, ולפיכך עליה להיות אישית וסודית.

7.4. חל איסור למסור את שם המשתמש והסיסמא שלך לאדם אחר או להשתמש בשם משתמש וסיסמא של חבר קהילה אחר במהלך עבודתך.

7.5. חל איסור על שמירת הסיסמא במקום בו היא עלולה להיחשף.

7.6. בכל מקרה של חשיפת הסיסמא או חשד לחשיפתה, יש להחליף את הסיסמא מידית.

8. <u>עזיבת עמדת העבודה</u>

8.1. משתמש העוזב את עמדתו ינעל את מחשבו (CTRL+Alt+Delete).

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

8.3. יש לוודא כי לגורמים שאינם מוסמכים (עמיתים לעבודה, אורחים, ספקים, קהל), לא תהיה גישה לחומרים בסיווג חסוי .

8.4. יש לגרוס נייר משרדי חסוי שאין בו צורך וחובת השמירה שלו בהתאם לתקנות החוק הסתיימה .

9. <u>שימוש באינטרנט.</u>

9.1. חל איסור להעביר מידע שהינו חסוי באמצעות היישומים השונים שברשת האינטרנט, אלא עפ"י הנחיות הממונה אבטחת מידע במכון.

9.2. יש להימנע ממסירת פרטים אישיים וחל איסור למסור את כתובת האימייל של מקום העבודה בעת רישום לאתרי אינטרנט, למעט רישום לאתרים הקשורים לעבודה.

9.3. אין להירשם לאתרים או אפליקציות פרטיות ע"י ששימוש בכתובת הדואר של המכון וסיסמת המכון.

10. <u>שימוש נאות בציוד המשרד</u>

10.1. חל איסור לחבר או להכניס מדיה מגנטית פרטית של החבר קהילה או של גורם חיצוני שלא לצורך עבודה למחשבי המשרד (דיסק און קי, CD , DVD , HD חיצוני וכו').

10.2. חל איסור לחבר טלפונים סלולריים למחשבי המכון ,

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

10.4. חל איסור לשנות את הגדרות אבטחת המידע של המחשב.

11. <u>שימושים אסורים בתקשורת אלקטרונית</u>

11.1. חל איסור על הצגה מוטעית, טשטוש, הסתרה או החלפה של זהות משתמש או מערכת תקשורת אלקטרונית.

11.2. חל איסור על קריאה, חטיפה או חשיפה של תקשורת אלקטרונית של חבר קהילה אחר ללא רשות מאותו חבר קהילה.

11.3. חל איסור מפורש על שימוש בתקשורת האלקטרונית לכל אחת מהמטרות הבאות:

11.3.1. עיסוק בפלילים.

11.3.2. פעילות בלתי מורשית להשגת כסף או הפעלת עסק פרטי.

11.3.3. גישה לאחת ממערכות המחשב של המכון או כל המכון או גוף אחרים, ללא אישור מתאים.

11.3.4. הפצת מכתבי שרשרת, דואר זבל אלקטרוני או התכתבות דומה.

11.3.5. העברת מסרים מטרידים.

11.3.6. הורדה או אחסון של חומר (כולל תוכנה) המוגן בזכויות יוצרים ללא רישיון חוקי.

11.3.7. הפצת מסמכים פנימיים של המכון או סוגי תקשורת אחרים מחוץ למכון ללא אישור מתאים.

12. <u>שימוש במדפסות ובמכשירי פקס</u>

12.1. חבר קהילה אחראי לאסוף את החומר מהמדפסת מיד לאחר שליחתו להדפסה, על מנת לוודא כי החומר המודפס לא יילקח על ידי גורם לא מורשה.

12.2. העברת מידע בפקס – במידה ומתבצעת העברת מידע רגיש / סודי / חסוי בפקס נדרש לקבל אישור מגורם אחראי על המידע

12.3. במקרה של מכשיר פקס מרכזי, הנמצא בשטח ציבורי, יש להשגיח שהחומר הנכנס או היוצא לא יילקח על ידי אדם אחר.

13. <u>אבטחה פיזית</u>

13.1. יש לנעול את דלת המשרד בסוף יום עבודה.

13.2. בכל מקרה בו מזהה חבר קהילה גורמים שאינם מוכרים לו או מתנהלים בצורה חשודה באזורי העבודה השונים, יש לוודא את זהות הגורם וללוות לנקודה אליה צריך להגיע. בכל חשד לפעילות לא חוקית, יש לדווח מידית למנהל הישיר ולממונה ביטחון.

14. <u>דיווח על אירועי אבטחת מידע</u>

14.1. חבר קהילת וולקני המזהה אירוע / בעיית אבטחת מידע ידווח עליו באופן מידי לממונה אבטחת מידע ו/או נאמן אבטחת מידע ו/או לקב"ט .

14.2. סוגי אירועים עליהם יש לדווח:

עבירות אבטחת מידע הנעשות ע"י חבר קהילה/ת עצמו/ה ו/או חברים אחרים.

14.2.1. חשד לפריצות אבטחת מידע במערכות השונות ובמחשב האישי.

14.2.2. 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 תוכנן ומשמעותן ואת חובותיי על פיהן.
ידוע לי כי במידה ולא אמלא את חובותיי כאמור לעיל, עלולים להינקט כנגדי צעדים וסנקציות בהתאם לחוק ולנהלי המכון

שם: _____ תפקיד: _____

תאריך: _____ חתימה: _____