תמצית מדיניות אבטחת המידע של איחוד הצלה

1. רקע

- פעילותו התקינה של ארגון 'איחוד הצלה' (להלן: 'הארגון') מושפעת ותלויה ברמת הסודיות, השלמות, הזמינות, הכלילות (Integrity) או השרידות של המידע והנכסים שבאחריות הארגון.
- המידע, המערכות המנהלות אותו, האמצעים והציוד עליו הוא מושתת, מהווים נכס מרכזי וחיוני של הארגון ויש להגן עליהם כעל משאבים אחרים בעלי ערך הארגון.
- פגיעה במידע תוביל לנזקים העלולים לתת אותותיהם בהיבטים תפעוליים, טכנולוגיים וכספיים וכן להוביל לפגיעה בצנעת הפרט של אזרחי המדינה, לפגיעה במוניטין ובתדמית הארגון והמדינה.
- מדיניות אבטחת המידע מבוססת על סיכוני האבטחה הדינמיים תוך התאמה לצרכים התפעוליים והארגוניים של הארגון. העקרונות המונחים במדיניות אבטחת המידע מהווים בסיס לנהלי העבודה בתחומי אבטחת המידע השונים.
- מדיניות אבטחת המידע של הארגון נגזרת מתקן ניהול אבטחת המידע הבינלאומי ISO27799 ותקן ISO 27001: 2013.

2. מנהיגות ומחויבות הנהלה לנושא אבטחת מידע

- הנהלת איחוד הצלה (להלן: 'ההנהלה') רואה את ההגנה על המידע בהיבט של שלימות, זמינות ואמינות כנושא בעל חשיבות עליונה.
- הנהלת הארגון לוקחת על עצמה להוביל ולהנחיל את כלל הנושאים והפעילויות הנדרשות על מנת לממש הגנה ראויה על המידע כפי שמתחייב עפ"י דרישות החוק ותקן ISO 27799 ו- ISO 27001.
- הנהלת הארגון תקצה את המשאבים הנדרשים, על מנת להגן על המידע ועל הנכסים של הארגון ולעמוד בדרישות מערכת ניהול אבטחת המידע (מנא"מ) כפי שמתחייב בתקן ISO 27799 ו- ISO 27001.
- על עובדי ומתנדבי הארגון להיות מודעים לסיכונים של חשיפת מידע, לעשות את כל האמצעים כדי למנוע חשיפה ואם יתקלו באירוע חריג עליהם לדווח על כך לגורמי אבטחת המידע בארגון.
- מטרות אבטחת מידע בארגון
- ניהול מערכת אבטחת מידע איכותית תוך שיפור מתמיד.
- עמידה בדרישות הרגולציה ותקנות המחייבות את הארגון.
- זיהוי וטיפול במירב הסיכונים ואי ההתאמות המאיימות על סודיות, זמינות ואמינות המידע שבאחריות הארגון.

- הבטחת זמינות המידע אשר אגור ברשתות, מערכות המידע ובתשתיות, לצורך המשך פעילות רציפה של הארגון.
- הבטחת אמינות המידע לאורך כל תהליכי העבודה בארגון.
- שיפור חוסן רשתות ומערכות המידע שבאחריות הארגון בפני פגיעה בסודיות, זמינות ואמינות המידע כתוצאה מפעילות זדונית של גורם פנימי / חיצוני.
- יישום מעגלי אבטחה פיזית הנדרשים להגנת סודיות, אמינות וזמינות המידע שבאחריות הארגון.
- וידוא השמירה על סודיות, זמינות ואמינות במידע שבאחריות הארגון ונמצא אצל צד ג'.
- העלאת מודעות לאבטחת מידע של מנהלי, עובדי ומתנדבי הארגון.

3. <u>עיקרי שיטת הערכת הסיכונים</u>

- עקרונות מדיניות אבטחת המידע יתבססו על מערכת ניהול סיכונים, המזהה, מבקרת ממזערת או מונעת את סיכוני האבטחה העלולים להשפיע על המידע, מאגריו או מערכותיו.

4. <u>אחריות על אבטחת מידע בארגון</u>

- הנהלת הארגון הגדירה את הגורמים והמסגרות הארגוניות, אשר באחריותם ליישם את מדיניות אבטחת המידע בארגון:

4.1.1. ועדת היגוי לנושא אבטחת מידע – מגדירה את מדיניות ונהלי הארגון בתחומים הנוגעים לאבטחת מידע.

4.1.2. ממונה אבטחת מידע - ממונה אבטחת מידע בארגון אחראי על הניהול השוטף של ענייני אבטחת מידע בארגון.

4.1.3. נאמני אבטחת מידע – ההנהלה מינתה נציגות אבטחת מידע ביחידות הארגון השונות, על מנת להבטיח הטמעה מיטבית של מדיניות אבטחת המידע בכלל חלקי הארגון.

4.1.4. מנהלי, עובדי ומתנדבי הארגון - על כלל מנהלי ועובדי הארגון חלה אחריות אישית בכל הנוגע לשמירה על אבטחת המידע וחסיונו.

5. **<u>מחויבות הנהלה -</u>** על מנת לממש את אחריותה ומחויבותה של ההנהלה לנושא אבטחת המידע הוגדרו ונקבעו הכללים לטיפול בנושאים הבאים :

- אבטחה לוגית - האבטחה הלוגית מהווה את ה"שכבה" העיקרית והקרובה ביותר בהגנה על המידע המצוי במערכות המחשב והתקשורת. ממונה אבטחת מידע בארגון יתווה את רמת האבטחה הלוגית המחייבת עבור רכיביהן השונים של מערכות המחשוב והתקשורת. תיושם מדיניות הרשאות ובקרת גישה למידע בהתאם לתפקיד והצורך המקצועי.
- אבטחה פיזית - ייושמו הגנות ובקרות פיזיות, על מנת למנוע פעולות אשר תוצאותיה עשויות להיות חשיפה, גניבה, שינוי או הרס של מידע. אמצעי הגנה אלו יתאימו לרמת הסיווג של המידע.
- אבטחת משאבי אנוש – נקבעו עקרונות אבטחת מידע בכל הקשור לעובדי ומתנדבי הארגון, על מנת לצמצם את הסיכונים הנובעים מבעיות במהימנות עובדים, חוסר מודעות של עובדים או רצון מכוון של עובד לפגוע במידע האגור במערכות הארגון.
- פיתוח מאובטח – הוגדרו היבטי אבטחת מידע ששולבו בתהליכי פיתוח מערכות מידע.
- רכש וספקים – מיושמים היבטי אבטחת מידע בתקשורת ועבודה עם ספקים חיצוניים.
- גיבויים – בארגון הוגדרו תהליכים להבטחת אמינות, שלמות, זמינות וכלילות (Integrity) המידע, וזאת ע"מ להבטיח שסוגי המידע השונים הקיימים בארגון מזוהים, וכי דרישות גיבוי לכל סוג של מידע מוגדרות בהתאם לרגישות המידע .
- בקרת גישה – נקבעו כללים ועקרונות למתן גישה ולמערכות המידע ובקרה אחר התחברות לרשת.
- שילוב מנגנוני הצפנה – בארגון פותחו עקרונות לשילוב מנגנוני הצפנה במערכות הארגון, על מנת להגן על מידע רגיש מפני חשיפה ושינוי.
- עבודה מרחוק – בארגון נקבעו כללים והנחיות אבטחת מידע לגישת עובדי הארגון וגורמים חיצוניים לרשת הארגון מרחוק.
- אבטחת אמצעי מחשוב ניידים – מבוצע יישום העקרונות, השיטה, תהליכי העבודה והאמצעים ע"מ לאפשר שימוש מאובטח במחשבים נישאים /ניידים ולמנוע פגיעה בשלמות, אמינות, זמינות, סודיות ושרידות המידע המאוחסן על גבי מחשבים ניידים בארגון.

6. **הנהלת הארגון רואה בכלל המנהלים והעובדים שותפים מלאים למאמץ להגנה על המידע ומצפה לשיתוף פעולה ביישום המדיניות והכללים הנגזרים ממנה.**

7. בברכה,

_____ _____

משה טייטלבוים, מנכ"ל איחוד הצלה תאריך