נוהל מערכת ניהול אבטחת מידע

טבלת שינויים

מס"ד	מס' סעיף	מהות השינוי	תאריך	שם המאשר	חתימה

1. כללי

1.1. המידע האגור במערכות המידע של הארגון הנו משאב קריטי, עיקרי ובעל ערך מהותי לפעילות החברה. על כן, ההגנה על המידע, שמירתו, מניעת שיבושו ומניעת שימוש לא ראוי בו מהווים מטרה מרכזית עבור הנהלת החברה.

2. מטרה

2.1. להבטיח כי הארגון קובע, מיישם ומתחזק נהלים ורשומות המעידות על הגנת המידע של הארגון, שמירתו, מניעת שיבושו ומניעת שימוש לא ראוי בו, תוך התאמתו לדרישות תקן ISO 27001 .

3. חלות

3.1. נוהל זה חל על כל עובדי הארגון

4. הקשר של הארגון

4.1. הבנת הארגון והקשריו

4.1.1. המידע האגור במאגרי המידע, בארכיון ובמערכות המידע של הארגון הנו משאב קריטי, עיקרי ובעל ערך מהותי לפעילות הארגון, לניהול מוצלח של עסקיו ולקיומו. על כן, ההגנה על המידע, שמירתו, מניעת שיבושו ומניעת שימוש לא ראוי בו מהווים מטרה מרכזית עבור הנהלת הארגון.

4.1.2. בנוסף לערכיות המידע, לפעילות ולעסקי הארגון, תהליכים שונים וחלקים ניכרים ממנו חשובים גם ללקוחות הארגון המגבים זאת בהסכמים עם הארגון.

4.1.3. ככלל, פעילות הארגון תלויה באופן מלא בתפקוד מערך המחשוב שלו. פעולה תקינה של מערך המחשוב מותנית בתקינות ובזמינות המידע המעובד על ידו.

4.1.4. לשם שמירה על עקרונות אלו הארגון החליט להקים מערכת נהלים לניהול אבטחת מידע אשר תהיה זמינה לכל שכבות העובדים בארגון.

4.1.5. מערכת הנהלים וההוכחות ליישומם יהיו מתועדים כך שניתן יהיה לראות בכל רגע נתון האם המערכת פועלת כמצופה. הנהלים יעודכנו לפי הצורך וכן עם שינויים בתהליכים או לאחר שדרוג טכנולוגיות.

4.1.6. ניהול המנא"מ יהיה מבוסס על העיקרון של "ארגון לומד" תוך שימוש בכלים להשגת שיפור מתמיד בכל הקשור לניהול המנא"מ.

4.1.7.ניהול המנא"מ יעשה תוך עמידה בכל דרישות החוקים הישימים:

4.1.7.1. חוק המחשבים, תשנ"ה-1995

4.1.7.2. חוק הגנת הפרטיות, התשמ"א-1981

4.2. הבנת הצרכים והציפיות של בעלי העניין

4.2.1.הארגון יקבע את:

4.2.1.1. בארגון בעלי העניין שונים המשפיעים על לאופן שבו הארגון מתכנן, מממש, בודק ומשפר את מערכת ניהול אבטחת המידע שלו.

4.2.1.2. הבסיס לכל הפעילות היא על אחראי אבטחת מידע בארגון הפועל באופן עצמאי ומסתייע בקבלני משנה לביצוע העבודה.

4.2.1.3. המנמ"ר של הארגון הינו הגורם והסמכות העליונה אשר מאשרת את כל התהליכים אותם מתווה הדרג המבצע.

4.2.1.4. הארגון מחויב לעמוד בדרישות חוזיות מול הלקוחות ובדרישות חוק. דרישות אלו מהווים את הבסיס להגדרת תהליכי אופן הניהול והבקרה של המערכת לניהול אבטחת מידע.

4.3. הגדרת תחום מערכת הניהול

4.3.1.מערכת ניהול אבטחת המידע כוללת את כל הפעילויות הנעשות בארגון ניהול ואחזקת מערכות מים וביוב בעיר בני ברק.

4.3.2.מערכת ניהול אבטחת המידע בארגון מקיפה את הגורמים הבאים:

4.3.2.1. כל עובדי הארגון והעובדים מטעמו.

4.3.2.2. כל האתרים הפיזים של הארגון.

4.3.2.3. כל מערך המחשוב של הארגון.

4.3.2.4. כל המסמכים שברשות הארגון.

4.3.2.5. ממשקים הקיימים לארגון עם גורמי חוץ בפעילות ובעבודה השוטפת.

4.4. הקמת מערכת הניהול

4.4.1. אבטחת מידע מוגדרת כמכלול הפעולות והאמצעים הננקטים והמיושמים במערכות המידע, בין שהן עצמאיות ובין שהן משולבות עם מערכות אחרות, בכדי להגן עליהן מפני פגיעה בזמינותן ובשרידותן, מפני חשיפה ושינוי במזיד או בשוגג של המידע האגור בהן ומפני פגיעה בשלמות המידע ובאמינותו.

4.4.2. פעילות אבטחת המידע של הארגון תתמקד בארבעה עקרונות מרכזיים המוגדרים להלן:

4.4.2.1. סודיות: חשיפת המידע בפני מורשים בלבד.

4.4.2.2. שלמות: אמינות הנתונים המופקים ואגורים במערכות המידע, בלא ששונו, נמסרו או נמחקו/בוטלו ללא הרשאות מתאימות.

4.4.2.3. זמינות: מצב בו המידע הינו בר גישה ובר שימוש בהתאם לדרישה של משתמש מורשה.

4.4.2.4. שרידות: היכולת של מערכת למלא את תפקידה בזמן, למרות תקיפות, תקלות או תאונות.

4.4.3. מטרתה של פעילות אבטחת המידע בארגון הנה למנוע חשיפת מידע של ו/או על לקוחות הארגון לגורמים בלתי מורשים, וכן מניעת פגיעה בשלמות ובזמינות מידע זה. בנוסף, מטרת הפעילות הנה למנוע פגיעה בסודיות, שלמות, זמינות ושרידות המידע העסקי, העלול להשפיע על אופן ההתנהלות התקין של הארגון.

5. מנהיגות

5.1. מנהיגות ומחייבות

5.1.1. המחויבות למדיניות המנא"מ של הארגון חלה על כל עובדיו ובראשם ההנהלה הבכירה.

5.1.2. הנהלת הארגון מקנה לעובדים, ללקוחות, לבעלי העניין ולגורמים בלתי תלויים את הביטחון שמחויבותה לנושא אבטחת מידע והמשכיות עסקית אליה מתכוונת ההנהלה - אכן מושגת ונשמרת.

5.1.3. ההקפדה על עבודה שיטתית בהתאם לנהלים מהווה חלק חשוב בתרבות הארגונית של הארגון, והיא מועברת באופן שוטף לעובדים ע"י הצוות הניהולי.

5.1.4. הארגון מוצא את יישום המדיניות ע"י יישום מלא של קובץ הנהלים.

5.1.5.לשם עמידה בעקרונות אלו הארגון יקיים, יתעד ויתספק ראיות לפחות בשמונה מישורים כדלקמן:

5.1.5.1. העברת מסר לכלל עובדי הארגון לגבי חשיבות נושא אבטחת המידע והמשכיות עסקית וההכרח לעמוד בכל הדרישות התחיקתיות הרלוונטיות בעזרת הדרכות וישיבות עבודה.

5.1.5.2. קביעת מדיניות אבטחת מידע פומבית והפצתה לכל הגורמים בארגון.

5.1.5.3. הגדרת מטרות וקביעת תוכנית להשגת המטרות.

5.1.5.4. הגדרת תפקידים, אחריות וסמכות של כל הגורמים האחראים לניהול המנא"מ.

5.1.5.5. ניהול סקרי הנהלה וקבלת החלטות מעשיות.

5.1.5.6. קיום מבדקים פנימיים וביצוע פעילויות מתקנות אפקטיביות לממצאים העולים בהם.

5.1.5.7. הבטחת זמינותם של משאבים נחוצים בדי לעמוד במדיניות, במטרות ובדרישות.

5.1.5.8. הגדרת קריטריונים לקבלת סיכונים ברמות הקבילות.

5.2. מדיניות

5.2.1.מדיניות אבטחת המידע תחול על כל עובדי ומנהלי הארגון וכל התשתיות המוגדרות בקובץ הנהלים.

5.2.2.המדיניות תופץ על ידי הנהלת הארגון לכל העובדים ובעלי העניין.

5.2.3.מדיניות אבטחת מידע של הארגון:

- תאגיד מניב ראשון בע"מ מקיים מערכת ניהול אבטחת מידע בהתאם לדרישות תקן ISO 27001 מתוך שאיפה לעמוד בדרישות ההנהלה, הלקוחות, חוקים ותקנות ובסטנדרטים מקובלים בשוק, ולספק ללקוחות שירות אמין ומהימן.
- התאגיד יבצע את עבודתו תוך שמירה על חוקים ודרישות של לקוחות ורגולציה בתחומי אבטחת מידע.
- התאגיד מכיר בצורך ליישום מנגנוני ביטחון ואבטחת מידע בתחום פעילותו.
- הנהלת התאגיד תעשה את המרב לשם מניעת האפשרות למעילה או הונאה על ידי עובדי התאגיד או כל גורם אשר יש לו קשר עסקי עם התאגיד.

- התאגיד ינהל מערך דינמי לניהול סיכונים בתחום הבטחת המידע ויפעל בכל העת להקטין את הסיכונים בהתאם להתפתחות הפעילות. הסיכונים ינוהלו תוך קביעת קריטריונים ברורים לחומרתם כך שיהיה ניתן להשוות בין הסיכונים השונים.
- התאגיד ינקוט בכל האמצעים הנאותים כדי לשמור על חסיונו, שלמותו וזמינותו של המידע וכן בשביל להגן על המידע שלו ושל לקוחותיו, מפני הגעתו לגורמים לא מורשים מהתאגיד ו/או אף מחוצה לו.
- הנהלת התאגיד מחויבת לתהליך של שיפור מתמיד וקידום מערך ניהול הבטחת המידע.
- התאגיד יפעל להעלאת המודעות של עובדיו והעובדים מטעמו להיבטי אבטחת מידע, ויבטיח כי כל מידע בנושא המועבר ע"י עובדי התאגיד ישמר בסודיות ללא שיהיה חשש לאשמה או נקיטת פעולות מצד התאגיד.
- הנהלת התאגיד מחויבת ליצור תשתית להמשכיות עסקית במקרה של אירוע חריג או כל כשל אשר תמנע פעילות שוטפת של התאגיד ומתן שירות איכותי ואמין ללקוחות.
- המדיניות תיסקר ותאושרר ע"י הנהלת התאגיד אחת לשנה במסגרת סקר ההנהלה של החברה, ולאחר אירועי ביטחון מידע.

5.2.4.סקירת מדיניות אבטחת מידע תכלול בין היתר את הנושאים הבאים:

5.2.4.1. השינויים שנערכו בתשתית טכנולוגיות המידע של הארגון ,והשינויים הנובעים מהם בפרופיל הסיכונים של הארגון;

5.2.4.2. השינויים שזוהו בסביבה החיצונית המשפיעים גם הם על פרופיל הסיכונים של הארגון;

5.2.4.3. דרישות והסדרי הבקרות, הציות והביטחון העדכניים הנדרשים על פי החקיקה התקפה ,או על בסיס חקיקה או רגולציה חדשה;

5.2.4.4. תקדימים או נהלים מקובלים בארגון;

5.2.5.יעדי מסמך מדיניות אבטחת המידע

5.2.5.1. קביעת תפיסת ההנהלה את אבטחת המידע בארגון, ואישוש מחויבותו לנושא.

5.2.5.2. קביעת עקרונות מנחים ליישום אבטחת מידע בארגון, שעל בסיסם ניתן יהיה ליישם אמצעי אבטחה, ולאורם ניתן יהיה לבחון את רמת האבטחה הקיימת.

5.2.5.3. העלאת רמת המודעות של מנהלי הארגון ועובדיו לנושאי אבטחת מידע.

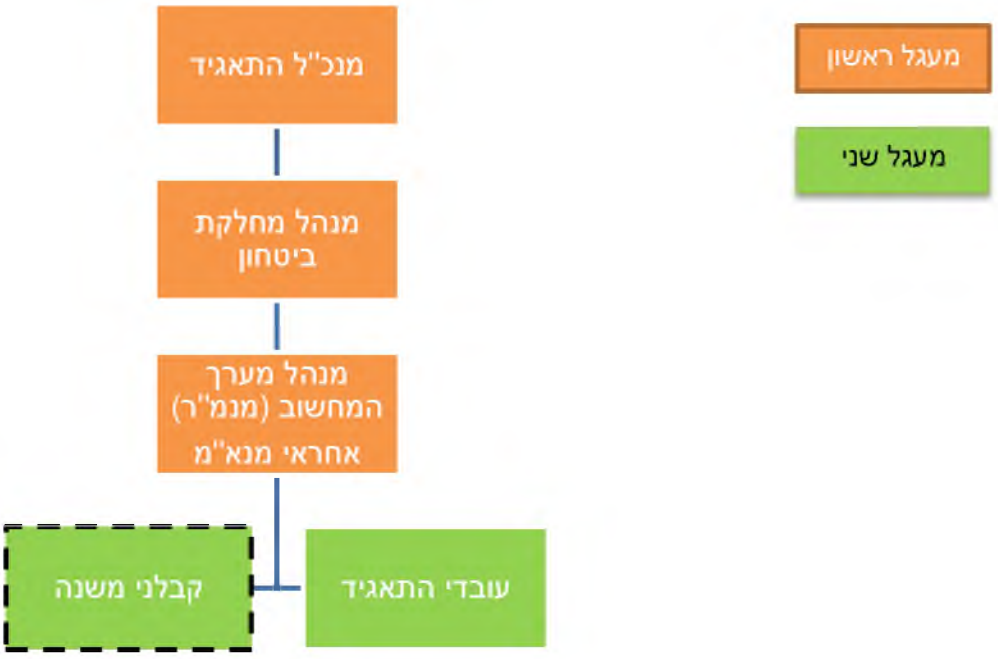
5.2.5.4. הגדרת סמכויות אבטחת מידע בארגון.

5.2.5.5. מתן מסגרת לתהליכים המרכזיים בארגון בנושאי אבטחת מידע, תוך יצירת תשתית לנהלים מקיפים בתחומים השונים. בסיס להגדרת היעדים הנוגעים לתחום המנא"מ.

5.3. תפקידים, אחריות, סמכויות

5.3.1. מבלי לפגוע בפעילות העסקית השוטפת ובמבנה הארגוני הנובע מפעילות זו, תוקמנה מסגרות ארגוניות אשר יישמו את מדיניות אבטחת המידע בארגון, ויבקרו את אופן יישומה. מסגרות אלה מגדירות את בעלי התפקידים השונים, את סמכויותיהם והיחסים ביניהם בתחום אבטחת המידע.

5.3.2. מבנה ארגוני של מערכת ניהול אבטחת מידע בארגון:



5.3.3.המנמ"ר הינו הסמכות העליונה והיחידה בכל הקשור לא"מ והוא בפועל מי שאחראי על הגדרת הדרישות ויישומן, ולכן הוא מוגדר בחברה גם אחראי מנא"מ.

5.3.4.תפקידי אחראי מנא"מ:

5.3.4.1. אחראי מערכת ניהול אבטחת מידע נושא באחריות ליישום בפועל של מדיניות אבטחת המידע של הארגון תוך פריטתה למטלות לביצוע, דרישות, הנחיות, נהלים וכלים טכנולוגיים. במסגרת זו, אחראי מנא"מ ינחה את כל הגורמים בארגון, בכל נושא בעבודתם שיש לו נגיעה לאבטחת מידע.

5.3.4.2. בנוסף יהיה אחראי על היישום בפועל של מדיניות אבטחת המידע בתחום האבטחה הפיזית של ציוד ומחשוב טכנולוגי ואבטחת מסמכים.

5.3.4.3. תפקידי אחראי מנא"מ כוללים:

5.3.4.3.1. הגדרת תכנית אבטחת מידע.

5.3.4.3.2. גיבוש ועדכון מדיניות אבטחת מידע.

5.3.4.3.3. הכנה והטמעה של נהלים, הנחיות עבודה ומתודולוגיות בנושאי אבטחת מידע.

5.3.4.3.4. ייעוץ להנהלה ויידועה בנושאי אבטחת מידע.

5.3.4.3.5. עדכון שוטף של נציג ההנהלה לאבטחת מידע.

5.3.4.3.6. טיפול באירועי אבטחת מידע.

5.3.4.3.7. הגדרת הסטנדרטים ליישום הטכני של אבטחת המידע במערכות הארגון.

5.3.4.3.8. ייזום דרישות לרכש של מערכות אבטחת מידע.

5.3.4.3.9. הגדרת דרישות אבטחת המידע בתהליכי פיתוח מערכות (חדשות או עדכון) ורכש ובקרה על יישומן במהלך הפרויקטים השונים.

5.3.4.3.10. הגדרת דרישות אבטחת מידע עבור תשתיות המידע.

5.3.4.3.11. העלאת מודעות עובדי הארגון לנושאי אבטחת מידע.

5.3.4.3.12. ביצוע בקרה על יישום מדיניות אבטחת המידע במערכות השונות ואיתור אירועים חריגים.

5.3.4.3.13. ביצוע סקרי סיכונים תקופתיים (סקרים כוללים או סקרים במערכות ספציפיות) הן פנימיים והן בלתי תלויים.

5.3.4.3.14. התעדכנות בטכנולוגיות אבטחת מידע ואיתור טכנולוגיות ומוצרים המתאימים לארגון.

5.3.4.3.15. אישור תוכנית אבטחת המידע, ואישור פעילויות החורגות מתוכנית האבטחה.

5.3.4.3.16. קביעת אמצעי ההגנה הפיזית בהתאם למיקום המערכת ורמת סיווג המידע אותו היא מכילה.

5.3.4.3.17. מניעת גישה פיזית על ידי גורמים שאינם מורשים למערכות ולמסמכים.

5.3.4.3.18. קביעת נהלי גישה מאובטחת לציוד ומערכות המכילות מידע.

5.3.4.3.19. קביעת נהלי גישה מאובטחת למסמכים המכילים מידע רגיש בהתאם למיקומו ולסיווג המידע.

5.3.4.4. בסמכותו של מנכ"ל התאגיד להאציל סמכויות של של אחראי מנא"מ לגורמים אחרים בתאגיד.

5.3.5. קבלני משנה

5.3.5.1. אחראים על יישום בפועל של חלק מתחומי אחריותו של אחראי מנא"מ בתחומי פעילותם ובהתאם למדיניות וכלים שנקבעו.

5.3.6.עובדי הארגון

5.3.6.1. עבודה ע"פ הנהלים שנקבעו.

6. תכנון

6.1. טיפול בסיכונים והזדמנויות

6.1.1.כללי

6.1.1.1. הארגון מעריך וקובע את הסיכונים בהם יש לטפל על מנת שהוא יוכל להשיג את המטרות שלשמן נכתב ומיושם קובץ הנהלים.

6.1.1.2. הטיפול בסיכונים של הארגון יבוצע באופן שוטף על מנת להבטיח כי הארגון משיג את המטרות שהציב לעצמו במסגרת המנא"מ.

6.1.1.3. הטיפול בסיכונים יעשה בכדי למנוע ככל הניתן השפעות לא רצויות ל פעילות ותפקוד הארגון.

6.1.1.4. הטיפול בסיכונים יעשה לאחר תכנון, תוך חתירה להשגת שיפור מתמיד במנא"מ ולעמידה במטרות והיעדים של הארגון.

6.1.2. **הערכת סיכוני אבטחת מידע**

6.1.2.1. הארגון יבצע הערכה של רמת הסיכון הנשקפת לכל אחת ממערכות המידע, המידע הפיזי, התוצרים והממשקים שברשותו. הערכת הסיכונים תתבסס על רמת הרגישות של כל מערכת ותתייחס למכלול סיכוני אבטחת המידע הפוטנציאליים.

6.1.2.2. הערכת הסיכונים תעודכן בהתאם לשינויים עסקיים, שינויי תשתית, סקירה תקופתית וע"פ החלטת אחראי מנא"מ.

6.1.2.3. אחראי מנא"מ ייזום סקרי סיכונים ובדיקות אבטחת מידע של מערכות שונות בארגון. מערכות בעלות סיווג גבוה ייסקרו באופן תקופתי בהתאם להנחיות ההנהלה. לגבי מערכות אחרות, אחראי מנא"מ, בשיתוף עם נציג ההנהלה, יקבע את תדירות הסקרים בהתאם לרגישות המערכת.

6.1.2.4. הסקרים יתבססו על ניתוח תהליכים עסקיים וייבחנו את יעילות אמצעי ההגנה שיושמו בארגון ואת רמת הגדרות אבטחת המידע במערכות המידע.

6.1.2.5. הארגון יזום סקרי אבטחת מידע לפני הטמעת שינויים משמעותיים במערכות בעלות סיכון גבוה.

6.1.2.6. בהתאם להערכת הסיכונים ייזום מנהל אבטחת המידע מהלך של ניסיונות חדירה מבוקרים למערכות המידע של הארגון

6.1.2.7. בדיקות אלו יבחנו את עמידותן של המערכות בפני סיכוני אבטחת מידע פנימיים וחיצוניים. תדירות מבחני החדירה תיקח בחשבון את רגישות המערך.

6.1.2.8. מבדקי החדירות יבוצעו בתדירות שתיקבע ע"י הנהלת החברה, על ידי גורמים מקצועיים עצמאיים, בלתי תלויים, חיצוניים לחברה, תוך מניעת ניגודי אינטרסים ונקיטת אמצעי זהירות מתחייבים.

6.1.2.9. הערכת הסיכונים תתבצע לפי המטריצה הבאה:

		הסתברות לאירוע		
		נמוכה	בינונית	גבוהה
השפעה של האירוע	נמוכה	נמוכה	נמוכה	נמוכה
	בינונית	נמוכה	בינונית	גבוהה
	גבוהה	בינונית	גבוהה	גבוהה
	קריטי	קריטי	קריטי	קריטי

סיכונים קבילים:
*רמת סיכון נמוכה – לא תהיה השפעה על אובדן מידע, הפרת סודיות או לפעילות העסקית
*רמת סיכון בינונית –השפעה מוגבלת שאינה גורמת לנזק על אובדן מידע או לפעילות העסקית. תיקון הנזקים ימשך זמן קצר.

סיכונים שאינם קבילים:
*רמת סיכון גבוהה – תהיה השפעה משמעותית על אובדן מידע, הפרת סודיות או לפעילות העסקית. תיקון הנזקים עלול להיות ממושך.
*רמת סיכון קריטית – נזק שאינו בר תיקון באמצעים סבירים ובמשך זמן סביר.

6.1.3. טיפול בסיכוני א"מ

6.1.3.1. ממצאי הסקרים ובדיקות החדירות ידווחו ויוצגו להנהלת הארגון ולגורמים מוסמכים נוספים במסגרת סקר ההנהלה. לגבי כל הממצאים שיאותרו יקבעו סדרי עדיפויות לטיפול ולוחות זמנים לסיום. באחריותו של אחראי מנא"מ לקיים מעקב בנדון ולוודא כי הוקצו לכך המשאבים הנאותים.

6.1.3.2. סיכונים שאינם קבילים (רמה קריטית וגבוהה) מחויבים להגיע לידיעת ההנהלה מיד עם גילויים. על אחראי מנא"מ לקבל אישור מפורש מההנהלה ביחס לסיכון כזה שאינו בטיפול מיידי.

6.1.3.3. עם סיום הטיפול בממצאים, יבצע אחראי מנא"מ בקרה על יישום ההמלצות.

6.1.3.4. במסגרת הטיפול בסיכוני אבטחת מידע ייושמו בקרות שונות בחברה. הבקרות יכולות להיות אותם הבקרות של נספח A של תקן ISO 27001 או בקרות אחרות. בכל מקרה, בקרות מהנספח שאינן מיושמות יהיו לאחר בחינה ומתן "הצדקה" לחוסר הצורך ביישום.

6.2. מטרות א"מ ותכניות להשגתן

6.2.1.הנהלת הארגון תגדיר מטרות ויעדים לאבטחת מידע.

6.2.2.המטרות והיעדים יקבעו על סמך תשתית הניהול שהוגדרה ותוצאות הסקרים והמבדקים שנערכים בארגון, ויתאימו לאופן מימוש הנהלים, ולמחויבות ההנהלה כפי שבא לידי ביטוי במדיניות אבטחת המידע.

6.2.3.המטרות והיעדים יוגדרו לפונקציות שונות וברבדים שונים במנא"מ.

6.2.4.המטרות והיעדים ידונו במסגרת סקר הנהלה ויאושרו ע"י הנהלת הארגון.

6.2.5.לכל יעד ו/או מטרה יקבעו לפחות הדברים יבאים:

6.2.5.1. מה ייעשה

6.2.5.2. משאבים הנדרשים

6.2.5.3. אחראי

6.2.5.4. תאריך היעד לסיום

6.2.5.5. אופן ביצוע הערכת תוצאות התהליך

7. תמיכה

7.1. משאבים

7.1.1.על מנת לקיים מערכת איכות מפנה הארגון משאבים שונים וכוח אדם מיומן.

7.1.2.האמצעים:

7.1.2.1. פונקציה של אחראי מנא"מ בארגון.

7.1.2.2. קיום מבדקים פנימיים (המבדקים יתקיימו באופן סדיר כדי להבטיח עמידה בתקן).

7.1.2.3. כלים לאיסוף נתונים, תיעוד.

7.1.2.4. כלים ותוכנות לביצוע העבודה.

7.1.3.כוח אדם:

7.1.3.1. אחראי מנא"מ.

7.1.3.2. שעות עבודה של ההנהלה וביצוע סקרים ומבדקים.

7.1.3.3. קבלני משנה ליעוץ ולביצוע סקרים.

7.1.3.4. משאבים לזיהוי דרישות תחיקתיות ודרישות של לקוחות.

7.1.4.תקציב:

7.1.4.1. הסכם הסמכה שנתי עם גוף התעדה.

7.1.4.2. תקציב להעסקת עובדים וקב"מ.

7.1.4.3. תקציב להדרכה ולשעות הדרכה ע"י גופים פנימיים וחיצוניים.

7.2. כישורים

7.2.1. הארגון יאייש (ישים) את עובדיו בתפקידיהם המוגדרים על סמך הסמכה, השכלה, ניסיון, כישורים ומיומנות כדלהלן:

7.2.2. אחראי מנא"מ - בעל ראיה רוחבית של תפקוד הארגון, בתפקיד ניהולי בכפוף לדרגים בכירים בארגון והכשרה מתאימה בתחום אבטחת המידע ע"י הדרכות חיצוניות ואישיות, לימוד עצמי וכדו'.

7.2.3. עורך מבדק איכות פנימי – נציג פנימי או חיצוני של הארגון אשר יש לו את הידע והניסיון בעריכת מבדקים ע"י הדרכות חיצוניות או לימוד עצמי.

7.2.4. השמת העובדים לתפקידיהם במערכת ניהול אבטחת מידע תיעשה רק כאשר עמדו בקריטריונים שהוגדרו לעיל.

7.2.5. הדרכה

7.2.5.1. הארגון יגדיר לכל תפקיד המשפיע על נושא אבטחת מידע קריטריונים ברורים להכשרה במסגרת התפקיד, רק עובדים אשר עמדו בקריטריונים אלו יוכלו למלא תפקידים אלו.

7.2.5.2. אחראי מנא"מ יבנה תוכנית להדרכת עובדים החל מהדרג הניהולי וכלה בדרג התפעולי.

7.2.5.3. ההדרכה תתבסס על זיהוי הצרכים בארגון תוך התאמה לאופי הארגון והעובדים התוכנית תאושר ע"י אחראי מנא"מ ותבוקר על ידו שאכן היא מבוצעת.

7.2.5.4. ההדרכות יתועדו והחברה תשמור רשומות הדרכה הכוללים את היקף בשעות, משתתפים, חומר להדרכה וכיו"ב.

7.2.5.5. אחראי מנא"מ יערוך מעקב אחר ביצוע ההדרכה ובמידה ויזהה פערים ישלים אותם לעובדים שלא הודרכו במועד שתוכנן.

7.2.5.6. הארגון יעריך את אפקטיביות ההדרכות באמצעים שונים כגון משובי הדרכה, תשאול עובדים במהלך מבדקים פנימיים וניתוח אירועים.

7.2.5.7. נושאי הדרכה יהיו לפחות הנושאים הבאים:

7.2.5.7.1. נהלי המנא"מ.

7.2.5.7.2. מדיניות המנא"מ.

7.2.5.7.3. אירועים שהיו בארגון.

7.2.5.7.4. מטרות ויעדים בתחום המנא"מ.

7.2.5.8. מדריכים: גורמי פנים, בעלי הניסיון וההכשרה המכסימלית כמו אחראי מנא"מ, מנהל רשת, וגורמי חוץ כמו יועצים חיצוניים.

7.2.5.9. הארגון ישמר את רשומות ההשמה וההדרכות בהתאם לשמירת רשומות איכות, כך שיתאפשר מעקב אחר ההשכלה, הניסיון וההדרכות.

7.2.5.10. הארגון ירענן, תקופתית, את הנהלים לכלל העובדים בכדי להעלות את מודעות העובדים לחשיבות עבודתם ותרומתם להשגת מטרות המנא"מ.

7.2.5.11. עובד חדש בארגון, כחלק מתקופת הניסיון וההכשרה שלו, יעבור הדרכה והכשרה להתאמה ולהכרה של נהלי המנא"מ של הארגון, באחריות אחראי מנא"מ ו/או המנהל הישיר.

7.2.5.12. במידה ונדרש עבור תפקיד מסוים הכשרה ע"פ חוק או תקן, יהיו אלה חובה לפני העסקת העובד בתפקידו. אחראי מנא"מ יוודא הכשרתו של העובד טרם שיבוצו לתפקיד.

7.2.5.13. הסכם הקליטה של עובדי החברה יכלול התייחסות לענישה אפשרית כאשר מזוהה הפרה של מדיניות ביטחון המידע.

7.3. הערכת סיכוני א"מ

7.3.1. הארגון יעביר מסר ברור לכלל העובדים והעובדים מטעמו ביחס לאחריותם האישית להצלחת יישום מערכת ניהול המנא"מ.

7.3.2. העברת המסר תכלול את ההתייחסות לאופן ההשפעה שלהם על אבטחת המידע בארגון, וההשלכות של אי התאמות שיכולים להיות תוצאה של התנהגותם.

7.3.3. הארגון יעביר לעובדים והעובדים מטעמו את מדיניות א"מ שלו.

7.4. טיפול בסיכוני א"מ

7.4.1.הארגון יחזיק רשימה עדכנית של אנשי קשר לשגרה, שעת חירום או גילוי אי התאמות.

7.4.2.הרשימה תכלול את הפרטים הבאים:

7.4.2.1. המידע המועבר/הנושא

7.4.2.2. הגורם המטפל

7.4.2.3. דרכי ושעות ההתקשרות עם הגורם המטפל.

7.5. מידע מתועד

7.5.1.כללי

7.5.1.1. הארגון ישמור רשומת המעידות על ביצוע דרישות של נהלים, הוראות וכדו'. מטרתם של רשומות אלו היא להראות את הקשר החד ערכי והעקיב שבין תכנון הפעולות לביצועם, תוך שילוב של ההחלטות והמדיניות של ההנהלה.

7.5.1.2. התיעוד יכלול את המסמכים הבאים:

7.5.1.2.1. תכנית טיפול סיכונים

7.5.1.2.2. כישורי אנשים המבצעים עבודה המשפיעה על ביצועי א"מ

7.5.1.2.3. תוצאות הערכת הסיכונים

7.5.1.2.4. תוצאות טיפול בסיכונים

7.5.1.2.5. תוצאות ניטור ומדידה של המנא"ם

7.5.1.2.6. תכנית מבדקים פנימים

7.5.1.2.7. תוצאות המבדקים

7.5.1.2.8. תוצאות סקרי הנהלה

7.5.1.2.9. אי התאמות ותוצאות פעולות מתקנות

7.5.1.2.10. רשימת מצאי נכסים

7.5.1.2.11. כללים לשימוש מקובל בנכסים

7.5.1.2.12. מדיניות בקרת גישה

7.5.1.2.13. דרישות לחיסיון והסכמי חיסיון

7.5.1.2.14. חוקים,דרישות חוזיות,תקנות וגישת הארגון לנושא

7.5.1.2.15. מדיניות ניהול מפתחות

7.5.1.2.16. לוג של אירועים

7.5.1.2.17. נוהל ניהול ותגובה לאירוע

7.5.1.2.18. נוהל טיפול במדיה נתיקה

7.5.1.2.19. נוהל סילוק מדיה

7.5.1.2.20. תהליך רישום והסרת משתמשים

7.5.1.2.21. תהליך הקצאת והסרת הרשאות

7.5.2.יצירת ועדכון מידע מתועד

7.5.2.1. הנוהל מתייחס לכל התיעוד המבוקר בארגון: מפרטים, הוראות עבודה, נהלים, תרשימים ורשימת נספחים כמפורט.

7.5.2.2. מספור הנהלים והסעיפים: המבנה הוא: IS- X.Y.Z.N.N.N.N

IS– מציין שהנוהל שייך למערכת ניהול אבטחת מידע (Information security)

X - מציין את המספר המוביל כפי שמופיע בתקן ISO 27001

Y - הנו מספר הנושא הפנימי של נוהל X.

Z - הנו מספר רץ בתוך הנושא המציין את מספרו הסידורי של הנוהל בתוך הנושא המוגדר.

N - הנו מספר רץ בהתאם לרמת הרשימה במסמך.

לדוגמא: נושא של יצירת ועדכון מידע מתועד ממוספר בתקן כ 7.5.2 ולכן הוא ימוספר בנהלי החברה כ X=7, Y=5, Z=2, N=0.

7.5.2.3. מספור נספחים: הנספחים ימוספרו באופן הבא: X.Y.Z.V כאשר X מציין את המספר המוביל של הנוהל, Y מציין את המספר של הסעיף בנוהל, Z מציין את המספר של הטופס לסעיף ו-V מציין את המהדורה.

7.5.2.4. מספור הוראות עבודה ונהלים פנימיים: בהתאם למספר הסעיף מנספח A של התקן.

7.5.2.5. כל נוהל והוראה פנימית יעבור בקרה לפני שיפורסם. נהלים יפורסמו עם חתימת אחראי מנא"מ ו/או נציג מההנהלה הבכירה בלבד. {חתימה יכולה להיות פיזית או העלאה לרשת המחשוב תחת המשתמש הייחודי של הגורם האמור}.

7.5.2.6. סקירת מסמכים תיעשה פעם בשנה במסגרת מבדק פנימי. לאחר הסקירה הם יאושררו.

7.5.2.7. המסמכים המעודכנים יוחזקו במחשב באחריותו של אחראי מנא"מ.

7.5.2.8. שינויים שנעשים באופן ידני על גבי מסמכים יעשו באופן בולט תוך ציון תאריך השינוי וגורם שביצע את השינוי. מסמכים אלו ישמרו גם לאחר סילוקם.

7.5.2.9. מסמכים פגי תוקף ישמרו בתיקיה ייעודית במחשב. מסמכים ששונו ידנית יסרקו לתיקיה זו.

7.5.2.10. הארגון יחזיק עותק קשיח מעודכן של המסמכים.

7.5.2.11. מסמכים שאינם קריאים יסולקו באופן מיידי.

7.5.2.12. מסמכים שהגיעו ממקורות חיצוניים יזוהו לפי מקור המסמך ותאריך העריכה שלו.

7.5.2.13. אחראי מנא"מ יפיץ את המסמכים למי שצריך בהתאם להרשאות ותוכן המסמך.

7.5.3. טיפול בסיכוני א"מ

7.5.3.1. כל התיעוד בארגון נגיש בכל עת לכל הגורמים המורשים לגשת אליו.

7.5.3.2. הארגון יגדיר הרשאות גישה שונות למערכות המחשוב ולנכסים פיזיים בארגון.

7.5.3.3. כל התיעוד הדיגיטלי בארגון ישמר באופן שבו כל שינוי במסמך מתועד ויש יכולת לבדוק מיהו הגורם שביצע את השינוי או לשחזר גרסה קודמת.

7.5.3.4. תיעוד אשר אין לשנותו (כגון קבצי PDF ,JPEG) ישמר בפורמטים המקוריים אשר אינם ברי שינוי.

7.5.3.5. הארגון יגדיר תיעוד שאינו ניתן למחיקה. תיעוד זה יהיה ניתן לעריכה לעובדים בכירים/מורשים, ולצפיה בלבד לשאר העובדים.

7.5.3.6. תיעוד פיזי יהיה נגיש לעובדים כפי שיוגדר. במידה והתיעוד "רגיש" הארגון יגביל את הגישה לתיעוד לאזורים מצולמים ו/או הגישה תהיה בנוכחות 2 אנשים לפחות.

7.5.3.7. זמן שמירת רשומות

7.5.3.7.1. שמירת רשומות חשבונאיות ומשפטיות: 7 שנים

7.5.3.7.2. שמירת רשומות איכות: 3 שנים

7.5.3.7.3. שמירת רשומות הקשורות לפעילות המוצר/שירות: 7 שנים

7.5.3.7.4. כאשר יש דרישות חוק ישמרו הרשומות בהתאם לדרישה.

7.5.3.8. חיסול רשומות

7.5.3.8.1. רשומות בעלי מידע המצריך חיסיון יגרסו ע"י הארגון.

7.5.3.8.2. במידה וקיימת דרישת לקוח לסילוק רשומות – יש לפעול לפי הדרישה.

7.5.3.8.3. רשומות איכות ללא מידע רגיש יושלכו לאשפה.

7.5.3.8.4. סילוק מצעים אלקטרוניים יעשה בהתאם להוראת העבודה שנכתבה לנושא.

8. תפעול

8.1. תכנון ובקרה תפעולית

8.1.1. בתכנון התהליך למימוש מנא"מ, הארגון מגדיר לכל תהליך מהם הדרישות עבור הגעה למצב בו נשמרת רמה גבוהה של אבטחת מידע ע"פ הדרישות בכמה אופנים:

8.1.2. הגדרת יעדים ומטרות לתחומי הפעילות השונים.

8.1.3. קיום ושמירת רשומות המעידות על ביצוע תהליכי מנא"מ כפי שהוגדרו.

8.1.4. קיום תהליך מסודר של בקרת ותיעוד השינויים בכל הרבדים של מערכת ניהול מנא"מ.

8.1.5. הגדרת תהליכי פיקוח ובקרה על פעולות הנעשות עבור הארגון במיקור חוץ.

8.2. הערכת סיכוני א"מ

8.2.1. הערכת הסיכונים תעודכן בהתאם לשינויים עסקיים, שינויי תשתית, סקירה תקופתית וע"פ החלטת אחראי מנא"מ.

8.2.2. אחראי מנא"מ ייזום סקרי סיכונים ובדיקות אבטחת מידע של מערכות שונות בארגון. מערכות בעלות סיווג גבוה ייסקרו באופן תקופתי בהתאם להנחיות ההנהלה. לגבי מערכות אחרות, אחראי מנא"מ, בשיתוף עם נציג ההנהלה, יקבע את תדירות הסקרים בהתאם לרגישות המערכת.

8.2.3. הארגון יזום סקרי אבטחת מידע לפני הטמעת שינויים משמעותיים במערכות בעלות סיכון גבוה.

8.3. טיפול בסיכוני א"מ

8.3.1. ממצאי הסקרים ובדיקות החדירות ידווחו ויוצגו להנהלת הארגון ולגורמים מוסמכים נוספים במסגרת סקר ההנהלה. לגבי כל הממצאים שיאותרו יקבעו סדרי עדיפויות לטיפול ולוחות זמנים לסיום. באחריותו של אחראי מנא"מ לקיים מעקב בנדון ולוודא כי הוקצו לכך המשאבים הנאותים.

8.3.2. סיכונים שאינם קבילים (רמה קריטית גבוהה) מחויבים להגיע לידיעת ההנהלה מיד עם גילויים. על אחראי מנא"מ לקבל אישור מפורש מההנהלה ביחס לסיכון כזה שאינו בטיפול מיידי.

8.3.3. עם סיום הטיפול בממצאים, יבצע אחראי מנא"מ בקרה על יישום ההמלצות.

8.3.4. במסגרת הטיפול בסיכוני אבטחת מידע ייושמו בקרות שונות בחברה. הבקרות יכולות להיות אותם הבקרות של נספח A של תקן ISO 27001 או בקרות אחרות. בכל מקרה, בקרות מהנספח שאינן מיושמות יהיו לאחר בחינה ומתן "הצדקה" לחוסר הצורך ביישום.

9. הערכת ביצועים

9.1. ניטור, מדידה, ניתוח והערכה

9.1.1. בקרה שוטפת

9.1.1.1. הארגון הקים מערך של בקרה לתהליכי הניהול השונים וכן לתשתית המחשוב בחברה.

9.1.1.2. מטרתו של מערך הבקרה הוא לגלות האם היישום של הנהלים, ההוראות והמשאבים המוקצים אכן נותנים מענה לדרישות אליהם מכוון הארגון.

9.1.1.3. אמצעי הבקרה יכלול אמצעים לגילוי וזיהוי של אירועים חריגים.

9.1.1.4. הארגון יבדוק את אפקטיביות מערך הבקרה שהוקם.

9.1.2.ניטור וסקירה של מנא"מ

9.1.2.1. הארגון יפעיל אמצעי בקרה ויסקור אותם במרווחי זמן מתוכננים על מנת שיוכל:

9.1.2.2. לזהות בזמן אמת ניסיונות של פריצה ותקריות אבטחה.

9.1.2.3. לזהות אירועים או גורמים שיכולים להתפתח לתקריות אבטחה.

9.1.2.4. לזהות שגיאות בתוצאות של עיבוד.

9.1.2.5. לקבוע האם פעולות שננקטו בעקבות אירועי פריצה היו אפקטיביות.

9.1.2.6. לתת להנהלה כלים לבדוק האם פעילויות האבטחה שהוטלו על אנשים או שיושמו באמצעי טכנולוגיית מידע מבוצעים כראוי.

9.1.2.7. הארגון יסקור אחת לשנה במסגרת המבדק הפנימי עם דיווח בסקר הנהלה את האפקטיביות של מנא"מ. הבדיקה תכלול התייחסות לתוצאות של מבדקי אבטחה, תקריות, תוצאות של מדידת אפקטיביות והצעות מכל בעלי העניין.

9.1.2.8. האפקטיביות תיבדק בכל נושא למול היעדים והמטרות שלשמם מוסדה הבקרה.

9.1.2.9. הערכות הסיכונים יבדקו בתדירות חצי שנתית ו/או עם שינוי ו/או גילוי של אחד הגורמים הבאים: שינויים בארגון, שיוניים בטכנולוגיה, שינויים במטרות העסקיות ובתהליכים העסקיים, שינויים באיומים שזוהו, שינויים באמצעי הבקרה, שינויים חיצוניים כמו שינויים בדרישות חקיקה ודרישות של לקוחות.

9.1.2.10. הארגון יבצע אחת לשנה מבדק פנימי שיכלול את כל הפעילויות שמסגרת מנא"מ.

9.1.2.11. במידה ונעשה שינוי באמצעי הבקרה ו/או שינוי אחר שיש לו השפעה על מערכת ניהול אבטחת המידע יערך מבדק פנימי בסמוך לשינויי לחלקים הרלוונטיים של מערכת ניהול האיכות.

9.2. מבדקים פנימיים

9.2.1. הארגון יקיים מבדקים פנימיים לבחינת אופן ניהול מנא"מ וזיהוי פערים בין הפעילות בפועל לבין דרישות ישימות כגון:

9.2.1.1. דרישת תקן ISO 27001 ונספחיו במהדורתו העדכנית.

9.2.1.2. דרישות ע"פ דין ואחרות שהארגון זיהה כישימות.

9.2.1.3. דרישות נהלי והוראות העבודה של תחום מנא"מ.

9.2.1.4. דרישות של לקוחות שהארגון התחייב לעמוד שהם.

9.2.2. המבדקים יערכו בתדירות שתיקבע ע"י אחראי מנא"מ , אך לפחות אחת לשנה.

9.2.3. אחראי מנא"מ יכין תוכנית לביצוע המבדקים. בעת הכנת התוכנית ילקחו בחשבון לפחות הנושאים הבאים:

9.2.3.1. תוצאות המבדקים הקודמים.

9.2.3.2. תוצאות מבדקים חיצוניים שנערכו.

9.2.3.3. שינויים שהיו במערכת ניהול המנא"מ.

9.2.3.4. שינויים בנהלים.

9.2.3.5. דרישות רגולציה ודרישות לקוחות.

9.2.4. התוכנית תכלול את כל תחומי הפעילות של מנא"מ כך שאחת לשנה לפחות יבדקו באופן מדגמי כל התחומים והפעילויות תוך כדי בדיקה של 100% מהנהלים והוראות העבודה.

9.2.5. עורך המבדק: נציג מטעם אחראי מנא"מ אשר מוכשר לכך (עובד חברה ו/או יועץ חיצוני). עורך המבדק לא יבדוק תחומי פעילות הנמצאים תחת אחריותו.

9.2.6. דוח המבדק

9.2.6.1. דו"ח המבדק הנו דו"ח על בסיס רשימת התיוג של מכון התקנים המותאם לצורכי ונהלי הארגון.

9.2.6.2. המבדק יתבצע בעזרת רשימת תיוג לצורך ביצוע המבדקים, רשימה המתאימה לצורכי הארגון.

9.2.6.3. הבודק מפרט ומגדיר מי נבדק במבדק ועל מה נבדק. כמו כן מפרט את מסקנותיו בדו"ח שכולל דגימות חיוביות ודגימות שליליות.

9.2.7. פעילות מתקנת להערות שהתגלו:

9.2.7.1. לאחר המבדק ירכז הבודק את ההערות במסמך שיועבר לאחראי מנא"מ לצורך קבלת תגובתו (ותגובת הנבדקים לפי הצורך) ולבחינה של הפעולות המתקנות הנדרשות.

9.2.7.2. אחראי מנא"מ יערוך חקירת שורש לכל אי התאמה שהתגלתה ויקבע את פעולת התיקון, לו"ז לביצוע, האחראי לביצוע, תאריך לבדיקת אפקטיביות ואופן בדיקת האפקטיביות.

9.2.7.3. בדיקת אפקטיביות תתבצע בהתאם ללו"ז שנקבע ע"מ לזהות האם הפעולות המתקנות שבוצעו היו אפקטיביות והאם הבעיה נפתרה.

9.3. סקר הנהלה

9.3.1.הנהלת הארגון מקיימת ישיבת סקר הנהלה אחת לשנה לפחות בהתאם למצב השוק, הארגון והלקוחות.

9.3.2.פירוט המשתתפים: נציג הנהלה, אחראי מנא"מ ומנהלים שונים לפי העניין.

9.3.3.מטרת ישיבת סקר הנהלה הנה להבטיח התאמה מתמדת ואפקטיבית של מנא"מ.

9.3.4.תשומות הסקר: הנושאים והנתונים שיובאו לדיון יהיו לכל הפחות:

9.3.4.1. תוצאות מבדקים, סקרים והערכת סיכונים של מנא"מ.

9.3.4.2. משוב מבעלי עניין.

9.3.4.3. מצבן של אי התאמות, הפעולות המתקנות והמונעות.

9.3.4.4. נקודות תורפה או איומים שלא זכו להתייחסות נאותה בהערכת הסיכונים הקודמת.

9.3.4.5. תוצאות של ניטור ומדידה.

9.3.4.6. פעולות מעקב מזמן עריכת סקר ההנהלה הקודם.

9.3.4.7. כל שינוי ארגוני, חיצוני או פנימי היכול להשפיע על מנא"מ, כולל הצורך בשינוי מדיניות/מטרות.

9.3.4.8. סטטוס פעולות מסקר הנהלה קודם.

9.3.4.9. המלצות לשיפור.

9.3.5.הנושאים דלעיל, הנם נושאים שעולים לדיון בכל סקרי ההנהלה. אלו למעשה נושאים קבועים המצריכים מאחראי מנא"מ להכין את האינפורמציה הדרושה מהמבדקים השונים ומתיקי התיעוד השונים. בנוסף לנושאים אלו מרכז אחראי מנא"מ נושאים נוספים רלוונטיים לסקר ההנהלה.

9.3.6. תפוקות הסקר: אחראי מנא"מ עורך פרוטוקול של הדיון ומתעד בו את נושאי הדיון, הממצאים, המסקנות והפעולות הנדרשות לביצוע. ההחלטות והפעולות הנדרשות לביצוע יהיו בתחומים הבאים:

9.3.6.1. שיפור האפקטיביות של המנא"מ.

9.3.6.2. עדכון הערכת הסיכונים והטיפול בסיכונים.

9.3.6.3. שינויים והתאמות בנהלים, הוראות עבודה ואמצעי בקרה.

9.3.6.4. צורך במשאבים.

9.3.6.5. שיפור באופן מדידת האפקטיביות של אמצעי הבקרה.

9.3.7. אחראי מנא"מ מציין את הסטטוס של ההחלטות הקודמות מדו"ח סקר ההנהלה האחרון.

9.3.8. אחראי מנא"מ מפיץ את הפרוטוקול לכל משתתפי הדיון ומתיקו בתיק סקרי ההנהלה.

9.3.9. בכל דיון יש לקבוע לכל היעדים פעולות לביצוע ולהם אחראי ליישום ולוח זמנים לבדיקת היישום. על הנהלת החברה להקצות את המשאבים הנחוצים לצורך יישום ההחלטות.

9.3.10. ממצאי סקר ההנהלה מופצים בקרב העובדים ע"י אחראי מנא"מ בדרכים הבאות: הסברה, הדרכה שיטתית, פרסום ותפוצה אישית.

9.3.11. אחראי מנא"מ משמש כקטליזטור לקיום סקר ההנהלה, דהיינו הוא יוזם את קיום הסקר במועדו.

9.3.12. אחראי מנא"מ אחראי לעקוב אחר ביצוע החלטות הסקר ולהביאם בפני משתתפי הסקר בישיבתם הבאה.

10. שיפור

10.1. אי התאמות ופעילות מתקנת

10.1.1. הגורמים המתניעים לפעולה מתקנת נובעים בין היתר מאי התאמה הנובעת מהמקורות הבאים:

10.1.1.1. אי התאמה לנהלים ו/או הוראות עבודה.

10.1.1.2. ליקויים במערך אבטחת המידע.

10.1.1.3. תלונות לקוחות.

10.1.1.4. אי יישום החלטות שהתקבלו בסקרי הנהלה.

10.1.1.5. תוצאות של מבדקי איכות פנימיים/חיצוניים.

10.1.2. פעילות מתקנת מבוצעת מיד עם גילוי ליקוי ו/או אי-התאמה.

10.1.3. אי ההתאמה שזוהתה תירשם בדו"ח הפעולה המתקנת תוך ציון התאריך והגורם האחראי.

10.1.4. אחראי מנא"מ בשיתוף הגורם האחראי לאי ההתאמה יבצע חקירת שורש לזיהוי הסיבה לאי ההתאמה.

10.1.5. לאחר ביצוע החקירה יחליט אחראי מנא"מ האם יש צורך בפעולה מתקנת רוחבית או שנדרש טיפול נקודתי בלבד. ההחלטה תתועד בטופס פעולה מתקנת.

10.1.6. פעילות מתקנת יכולה להיות בכל רבדי פעילות הארגון: החל בשינוי של נהלים והוראות עבודה ועד לשינויים במערך הטכנולוגי ושינויים בכ"א בארגון.

10.1.7. במידת הצורך אחראי מנא"מ יכנס את העובדים לשם הסברה והדרכה. אם מתבצעת הדרכה מסודרת יש לערוך פרוטוקול, לרשום שמות המשתתפים, תאריכים, שעות ומהם הנושאים שהועלו.

10.1.8. בטופס הפעולה המתקנת תתועד אופן בדיקת האפקטיביות של הפעולה המתקנת וכן מועד לבדיקה.

10.1.9. לאחר ביצוע הפעולה המתקנת אחראי מנא"מ יתייק את דו"ח הפעילות המתקנת לצורך מעקב לבדיקת האפקטיביות שלה.

10.1.10. אחראי מנא"מ יבצע בדיקה דו חודשית לסגירת הפעולות המתקנות.

10.1.11. במידה ונמצא כי פעולה מתקנת אינה אפקטיבית יש לתעד זאת וכן את ההחלטה בדבר הפעולה המתקנת החדשה.

10.1.12. רשומות הנוגעות לאי ההתאמה ולתהליך החקירה הינם רשומות איכות. יש לשמרם במקום נגיש לצורך בדיקת האפקטיביות ולמידה לעתיד.

10.2. שיפור מתמיד

10.2.1. הנהלת הארגון פועלת להשגת השיפור מתמיד בכל תהליכי העבודה של מנא"מ, לשם כך הנהלת הארגון תתכנן ותנהל תהליכים לשיפור מתמיד של מנא"מ.

10.2.1.1. שיפור מתמיד הנו שיפור באפקטיביות של המנא"מ.

10.2.1.2. ההתייחסות לשיפור מתמיד מתבצעת בכמה רבדים בארגון:

10.2.1.3. מדיניות אבטחת מידע.

10.2.1.4. מטרות אבטחת מידע.

10.2.1.5. תוצאות מבדקים.

10.2.1.6. ניתוח אירועים מנוטרים.

10.2.1.7. פעולות מתקנות.

10.2.1.8. פעולות מונעות.

10.2.1.9. סקרי הנהלה ויעדי מנא"מ.

10.2.1.10. שינויים במנא"מ

10.2.2. ברבדים לעיל, בחלקם ובאחרים יוגדרו ויתוכננו דרך הניהול לשיפור המתמיד והנקודתי, דרך ממצאים, נתונים וניתוחים.