## מדיניות אבטחת מידע

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| זכויות יוצרים “התאחדות לכדורגל” ©  מסמך זה והידע הכלול בו הינם הקניין הבלעדי של “התאחדות לכדורגל” ואינם ניתנים לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתקה במלואם ו/או בחלקם, במישרין, ו/או בעקיפין, ללא הסכמה מראש ובכתב של “התאחדות לכדורגל”.   * 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 ב”התאחדות לכדורגל”   נתונים כללים   |  |  | | --- | --- | | ערך: בוריס קוגן | | | 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 | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |

1. רקע:
   1. פעילותה התקינה והמוצלחת של “התאחדות לכדורגל” מושפעת ותלויה מרמת סודיות, שלמות, אמינות, עדכניות, זמינות ושרידות המידע.
   2. המידע, התהליכים והמערכות התומכות מהווים הנכס העיקרי ביותר של “התאחדות לכדורגל” ולכן יש להגן עליהם בכל דרך ואמצעי שהם.
   3. פגיעה במידע, במאגריו או במערכותיו, לרבות חשיפה, חבלה או שיבוש, עלולים לפגוע בפעילות ובתדמית “התאחדות לכדורגל”. בד בבד קיים בחברה מידע אישי רגיש מהיבט חוק הגנת הפרטיות, התשמ"א- 1981, של לקוחות החברה ועובדיה, כאשר פגיעה במידע זה או חשיפתו לגורמים לא מורשים מתוך החברה ו/או אף מחוצה לה, מהווה "עוולה אזרחית" לפי החוק והוראות פקודת הנזיקין [נוסח חדש] 3.
   4. “התאחדות לכדורגל” תגן על המידע, התהליכים ומערכות המעבדות ואוגרות אותו לפי המוגדר בחמשת מעגלי האבטחה המצוינים במדריך אבטחת מידע זה וכמפורט בקובץ הנהלים המצורף.
   5. אבטחת המידע ב"התאחדות לכדורגל” תיושם בכפוף ובצמידות לחוקים ישימים, חוקי מדינת ישראל הנוגעים לתחום אבטחת המידע, לרבות חוק המחשבים וחוק הגנת הפרטיות ותקנותיו, בכפוף לזכויות קניין אינטלקטואלי, זכויות יוצרים ובהתאם להחלטות פורום ההנהלה לנושא אבטחת מידע.
2. מטרה:
   1. מדריך אבטחת מידע זה מציין את העקרונות והקווים המנחים אשר קבעה ואימצה הנהלת “התאחדות לכדורגל”, המהווים תשתית לנוהלי והנחיות החברה בהיבט אבטחת מידע.
3. מסמכים ישימים:
   1. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
4. הגדרות:
   1. מידע: כל נתון הנוגע ו/או הקשור לפעילותה, תפעולה או תפקודה של “התאחדות לכדורגל” הקיים על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרונים, על-גבי מצעי מידע פיזיים וכן המועבר בעל-פה.
   2. אבטחת מידע: מכלול הפעולות והאמצעים הננקטים והמיושמים ב”התאחדות לכדורגל” שמטרתם להביא לכך שהמידע ופריטי הציוד היוצרים אותו ומטפלים בו, יוגנו מפני פגיעה, חשיפה או שינוי, במזיד או בשוגג, הן מתוכי החברה והן מחוצה לה.
5. ההנהלה
   1. מחויבות הנהלת “התאחדות לכדורגל” והחברות הבנות (להלן: "ההנהלה") :
   2. ההנהלה מחויבת כלפי מטרות ועקרונות אבטחת המידע ומכירה בחשיבות האבטחה כחלק בלתי נפרד מקיומה העסקית, תהליך אשר יזוהה וימופה תקופתית באמצעות "סקר סיכונים מקיף".
   3. ההנהלה, מתחיבת לעמוד בדרישות החוקים, המדיניות והנהלים הנגזרים, לרבות הוראה לניהול סיכוני אבטחת מידע בענף הביטוח והפנסיה .
   4. ההנהלה תקיים ישיבות סדירות מידי תקופה בה ידונו נושאי אבטחת מידע שוטפים וחריגים (להלן: "סקר הנהלה").
   5. ההנהלה מחויבת להקצות את המשאבים הנדרשים לקיומם ההולם של הנהלים, התהליכים, השיטות והכלים הנגזרים ממדיניות ומדריך אבטחת מידע זה.
   6. ההנהלה תגדיר תפקידים ותחומי אחריות בכלל ובהיבטי אבטחת מידע בפרט.
   7. מנהל אבטחת המידע זיהה ומיפה את בעלי העניין הפנימיים והחיצוניים לנושאי אבטחת מידע בכלל רובדי החברה, תוך ציון הדרישות הייעודיות אשר משפיעות על האבטחה והמידע בחברה של כל אחד מהם.
   8. שותפים והנהלת החברה – מחויבים לתדמית החברה והמידע העסקי של הלקוחות והחברה.
   9. עובדים – מחויבים לחיסיון ושלמות המידע של החברה והלקוח.
   10. לקוחות – מגדירים לחברה את דרישות אבטחת המידע בהסכמים.
   11. גופי ממשל ורגולציה – על החברה לעמוד בדרישות הרגולטור הנוגעות לאבטחת המידע של הלקוחות ושל העובדים .
6. "חמשת מעגלי האבטחה":
   * + אבטחה פיזית.
     + אבטחת רשומות.
     + אבטחה לוגית (אבטחת המחשוב והתקשורת).
     + אבטחת מהימנות עובדים.
     + אבטחת ממשקים עסקיים.
   1. פעילותה התקינה והמוצלחת של החברה מושפעת ותלויה מרמת סודיות, שלמות, אמינות, עדכניות, זמינות ושרידות המידע והתהליכים התומכים:
      * חיסיון – הנהלת החברה מקיימת ומיישמת את ההגנות והבקרות הנדרשות למניעת חשיפת המידע והידע שלה ושל לקוחותיה אשר נמצא ברשותה, לגורמים לא מורשים בתוך החברה ומחוצה לה או אף שימוש על ידי גורמים עוינים.
      * מהימנות - החברה מעסיקה עובדים מהימנים ואמינים בהתאם לאמות מידה אשר נקבעו או נדרשו בתקנות, בחוקים ייעודיים ובהסכמים עם הלקוח.
      * זמינות - המידע אשר אגור במאגרי המידע של החברה יהיה זמין בכל עת למשתמשים מורשים בלבד, בעת שגרה וחירום.
      * תאימות – החברה מקיימת הליך של ניטור ובקרה לשם סקירת פעולותיה ומערכותיה, לבחינת מידת עמידתה בדרישות החוק, מדיניות אבטחת המידע אשר אימצה והנהלים הנגזרים ממנה, וכן למחויבות ללקוח.
7. ארגון אבטחת המידע – בעלי תפקידים:
   1. פורום הנהלה לנושא אבטחת מידע (באמצעות סקר הנהלה) - פורום ניהולי בראשותו של נציג דירקטוריון החברה, אשר נועד להתוות, לגבש ולעדכן את מדיניות “התאחדות לכדורגל” בתחום אבטחת המידע (להלן: "הפורום").
   2. מנהל אבטחת מידע: מנהל מערכות המידע, אשר בנוסף לתפקידיו הינו המנהל המקצועי של מערכת ניהול אבטחת המידע ב”התאחדות לכדורגל”.
   3. צוות ה- System : צוות מקצועי הכפוף למנהל מערכות המידע אשר מבצע הלכה למעשה את האמור בקובץ נהלים זה, ע"פ הנחיות מנהל אבטחת המידע ולפי התווית המדיניות של הפורום לנושא אבטחת מידע.
8. עבודה מרחוק ושימוש בהתקנים ניידים.

בחברה נקבעו כללים לשימוש במחשבים ניידים ובאפשרות עבודה מרחוק:

* 1. לפי מידת הצורך התפעולי, ובאישור של מנכ"ל החברה, מוקצה מחשב נייד לעובדי החברה ואפשרות עבודה מרחוק תוך התחברות מאבטחת באמצעות VPN.
  2. חל איסור מוחלט לאגור כל מידע מסווג (רגיש) במחשבים הניידים ובכל מדיה נתיקה שהיא. במקרים חריגים שמירת מידע במחשב נייד מתבצעת תוך ביצוע הצפנת המידע.

1. אבטחת משאבי אנוש:
   1. בחברה יועסקו עובדים אמינים, אשר יעברו הדרכות להעלאת מודעותם לנושאי אבטחת מידע בהתאם לתפקידם
   2. לפני העסקה:

החברה תבטיח שעובדיה ועובדי צד ג' (עובדי קבלן) מתאימים לתפקיד שיועד להם, מבינים את האחריויות המוטלות עליהם לשם מניעת מקרי כשל, הונאה או שימוש לרעה במידע ונכסי החברה והלקוחות:

* + - מהימנותם של עובדי החברה תיבדק לפני קליטתם באמצעות תשאול ממליצים ו/או באמצעות בחינה של גורם חיצוני, בהתאם לצורך התפקודי. במידת הצורך, יבוצע לעובד תחקיר ע"י קב"ט החברה.
    - כל עובד, בכל רמה היררכית שהיא, יחתום על הסכם שמירת סודיות וחיסיון NDA כתנאי לעבודתו בחברה.
    - לפני התחלת העבודה יעבור העובד החדש הדרכה להכרת החברה ונוהלי האיכות ואבטחת המידע בפרט.
    - הנהלת החברה נוקטת את מירב האמצעים לשם קליטת עובדים מהימנים ואמינים.
  1. במהלך ההעסקה:
     + החברה תבטיח שעובדיה ועובדי צד ג' מודעים לאיומי אבטחת המידע, לאחריות ולסמכות המוטלת עליהם, ושמדיניות אבטחת המידע והנהלים הנגזרים ממנה ידועים להם, לשם מניעת כל כשל באבטחת מידע בשוגג או בזדון.
     + מנהל אבטחת מידע יקיים הדרכות תקופתיות לכל עובדי החברה בכל רובדי החברה להעלאת המודעות לנושאים הבאים:
       - מדיניות אבטחת איכות ואבטחת מידע
       - הכרת סיכונים ואיומים אפשריים על החברה והמידע.
       - שימוש נאות ואתי בנכסי החברה.
       - אופן ההתגוננות מפני כשלים אפשריים.
       - אופן ההתנהגות בעת קרות אירוע חריג ותלונת לקוח.
       - שימוש נאות ונכון בהגנות ובבקרות.
       - עשה ואל תעשה במידע ובמערכות התומכות בו.
       - שירותיות ותקשורת עם הלקוח.
     + עובדים אשר עוסקים בתחום אבטחת מידע, יהיו בעלי הסמכות וכישורים יעודיים לנושא.
  2. סיום העסקה או החלפת תפקידים:

באחריות החברה להבטיח שעובדיה, עובדי חוזה או משתמשי צד ג' במערכות המידע יעזבו את הארגון או יחליפו תפקידים באופן מסודר ובטוח.

* + - בעת מעבר מתפקיד לתפקיד באחריות הצוות הניהולי של החברה לוודא כי מהימנותו ואמינותו של העובד אכן מתאימים לתפקיד החדש.
    - בעת מעבר בין תפקידים יש לתת את הדעת להרשאות ולבקרות הגישה אשר היו לעובד בתפקיד הקודם מול ההרשאות החדשות המוקצות לו. כברירת מחדל, יחסמו ההרשאות של התפקיד הישן, ותפתחנה לעובד הרשאות חדשות התואמות את התפקיד החדש.
    - עם עזיבת עובד את החברה, מסיבה כלשהיא, על הצוות הניהולי לוודא כי:
      * נחסמו כל אפשרויות הגישה שלו למידע, למערכות התומכות ולנכסים מהחברה או מחוצה לה.
      * העובד החזיר את כל הנכסים השייכים לחברה (ציוד, מידע וכדומה).
      * העובד קיבל הדרכה בדבר מחויבותו למידע וחסיונו.
    - באישור מנכ"ל החברה / מנהל אבטחת מידע, ניתן יהיה להעביר תוכן תיבת דואר אלקטרוני של עובד שעזב לעובד אחר.

1. ממשק עסקי & שירותי גורם צד ג' – אבטחה:
   1. בחברה מועסקים עובדים מעטים אשר אינן נמנים על העובדים הקבועים של החברה כמו עובדי ניקיון ועובדי תחזוקה מזדמנים, גורמים אלה אינם אמורים להיחשף למידע המצוי בחברה ו/או אצל לקוחותיה.
   2. הנהלת החברה תקבע את הגנות והבקרות הנדרשות, ראה נוהל ממשק עסקי צד ג.
   3. העסקת קבלני משנה ע"י החברה תהייה בהתאם לנוהל רכש.
2. סיווג מידע:
   1. הנהלת החברה תגבש קווים ואמות מידה להגדרה וסיווג רגישות המידע וחיוניותו, בהתאם לרמת הסיכון והנזק שייגרם ל”התאחדות לכדורגל”, כתוצאה מחשיפה, חבלה או שיבוש של המידע, מאגריו או מערכותיו, בין אם במזיד ובין אם בשוגג.
   2. סיווג המידע יקוים בכל אופן בו המידע אגור ושמור בכל מצע מידע שהוא (קבצים, בסיסי נתונים, מדיה אלקטרונית או אופטית, מסמכים, דו"חות וכדומה).
   3. סיווגו של המידע יקבע בהתאם לרמת הרגישות הגבוהה ביותר הקיימת בקובץ, במאגר או במצע הפיזי בהם אגור המידע (על-פי עקרון "המחמיר קובע").
3. רמת האבטחה:
   1. באחריות מנהל אבטחת המידע לקבוע את רמת האבטחה בהתאם לרמת הסיכון והרגישות שנקבעה ובכפוף לאישור הפרום.
   2. רמת האבטחה תקיף ותכסה את המידע בכל מעגלי האבטחה.
   3. רמת האבטחה בכל מערכות המידע ומצעי המידע, לא תהיה פחותה מרמת האבטחה של המידע בסיווג הגבוה ביותר האגור בה.
   4. רמת אבטחת המידע בכל המערכות ומתקני “התאחדות לכדורגל” תהייה בהתאם לרמת האבטחה הגבוה ביותר שתקבע.
4. ניהול וסיווג סיכונים:
   1. עקרונות אבטחת המידע יתבססו על סקר סיכונים תקופתי, אשר יזהה וימפה את התהליכים והנקודות אשר עלולים להשפיע על המידע, מאגריו או מערכותיו.
   2. ניהול הסיכונים יהיה מושתת על הערכת סיכונים המשקפת את מידת פגיעותם של המידע, מאגריו ומערכותיו, הערכת האיומים, השלכותיהם ומידת היתכנות התממשותם.
   3. פורום ההנהלה לנושא אבטחת מידע יגדיר את עקרונות סיווג המידע אשר יתבססו על חוקי המדינה והתקן לניהול אבטחת מידע ת"י 27001 Iso.
   4. מנהל אבטחת המידע יגדיר, את התהליכים והכלים הנדרשים לאבטחתם של נכסי החברה בכלל והחברות בפרט, בהתאם להערכת הסיכונים ולסיווג המידע אשר אגור ומעובד בהם.
5. אבטחה פיזית:
   1. מעגל אבטחה זה הינו המעגל החיצוני אשר נותן מענה ראשון להגנה בפני גורמים עוינים לחברה. קב"ט החברה יתווה את עקרונות הטיפול וההגנה הנדרשים. תחומי התייחסות:
      1. שיטות וכלים למידור עובדי ואורחי החברה.
      2. דרישות מבנה ותנאים סביבתיים ופיזיים.
      3. הרשאות גישה לרכיבי המערכת השונים, לרבות מחשבים וציוד תקשורת.
      4. תהליכים ואמצעים לפיקוח, בקרה ואכיפה.
      5. טיפול באירוע חריג.
6. טיפול במצעים:
   1. על עובדי החברה חל איסור לאגור כל מידע של החברה במצעי מידע נתיקים וניידים.
   2. מצעי מידע (מסמכים ומדיות) המכילים מידע ברמות סיווג שונות מוגנים באופן פיזי ולוגי מפני הגעה וחשיפה לגורמים לא מורשים מקרב עובדי החברה או חיצוניים לו.
   3. מצעי המידע מוגנים מפני כל אפשרות של פגיעה בשלמותם ופגיעה באמינות המידע אשר אגור בהם.
   4. באחריות כל עובדי החברה בכל רמה היררכית שהיא, לרבות עובדי צד ג', להשמיד או להשליך למכלים ייעודיים כל מצע מידע (מסמכים ומדיות) אשר מכילים מידע חסוי או רגיש כפי שהוגדר במדיניות זו, לשם השמדה.
7. אבטחת ציוד:
   1. הנהלת החברה מקצה את המשאבים הנדרשים על מנת למנוע כל פגיעה או נזק לציוד בכלל ולמערכות המחשב בפרט.
   2. התקנה, טיפול ותחזוקת מערכות מחשוב ותקשורת מתבצע על ידי נציגי ה It בלבד או עובדי צד ג' מוכרים ומוסמכים לבצע את המוטל.
   3. ציוד מערכות מחשב ותקשורת בכלל וציוד המכיל מידע בפרט, אשר אין צורך בו יושמד ללא כל אפשרות אחזור המידע שבו.
   4. מערכות החשמל והתקשורת בחברה מוגנות באמצעים מיוחדים לשם מניעת כל פגיעה בהם ובתשתיות שלהם, וכן למניעת חדירה דרכם לתשתיות תקשורת רגישות על ידי עובדי החברה או חיצוניים לה.
8. בקרת התיעוד:
   1. מערכת ניהול אבטחת המידע וכל פעילות הכרוכה בכך תהיה מתועדת על פי הנדרש במערכת ניהול האיכות ובנהלים הייעודיים.
   2. המסמכים אשר משמשים את מערכת ניהול אבטחת המידע יהיו מתועדים ומבוקרים כנדרש.
   3. התיעוד ישמר על גבי מצעים פיזיים ו/או מגנטיים בהתאם למצוין בנוהל הייעודי.
9. אבטחת רשומות:
   1. רשומות מידע כוללות מצעי מידע פיזיים כגון מסמכים, דיסקים, DOK, קלטות .
   2. אבטחת הרשומות תמנע הגעתן לידי גורמים לא מורשים בתוך “התאחדות לכדורגל” ומחוצה לה.
   3. פורום ההנהלה לנושא אבטחת מידע יתווה את קווי הפעולה ועקרונות אבטחת הרשומות בכל אופן אשר הן מופיעות.
   4. מנהל אבטחת המידע יגדיר את אמצעי ותהליכי הטיפול באבטחת הרשומות, בהתאם לרגישות וסיווג המידע ובהתאם לאופי החברה.
   5. תחומי ההתייחסות:
      1. שיטות וכלים לאבטחת מידע והשמדתו, בהתאם לסיווג המידע.
      2. תהליכי ואמצעי שינוע מידע (פנים וחוץ ארגוני).
10. אבטחת המחשוב והתקשורת (אבטחה לוגית):
    1. מעגל אבטחת המחשוב והתקשורת, האבטחה הלוגית, מהווה מעגל ההגנה העיקרי על המידע והתהליכים המצוי במערכות המידע ורשתות התקשורת של החברה.
    2. יישום נכון ונאות של כלי ותהליכי האבטחה במעגל זה, ימנע הגעת מידע לגורמים לא מורשים מהחברה ומחוצה לה, וכן גרימת נזק בשוגג או במזיד ע"י אותם גורמים.
    3. תיושם הגנה לוגית במערכות ההפעלה, בתוכנות ובמערכות התפעול, בקבצי ובמסדי הנתונים, בפעולות שינוי נתונים ובתקשורת, בכפוף לחוקים, תקנות ונוהלי אבטחת המידע של החברה.
    4. באחריות מנהל אבטחת המידע להתוות ולהגדיר את עקרונות הטיפול באבטחה הלוגית, לספק ולתחזק את האמצעים הדרושים לקיום פעילות האבטחה, בהתאם להחלטות פורום ההנהלה.
    5. תחומי התייחסות:
       1. שיטות וכלים לאבטחת מידע במערכות המחשב והתקשורת, בהתאם לסביבות העבודה ולהגדרות הפרופילים שיקבעו.
       2. הטמעת נהלי אבטחת מידע בקרב עובדי החברה וממשקיה העסקיים.
       3. תהליכים ואמצעים לפיקוח, בקרה ואכיפה.
       4. טיפול בחריגים.
11. אבטחת התקשורת:
    1. יקוים עקרון הריכוזיות בקישור מערכות החברה אל ומחוצה לה (שערי כניסה ויציאה מוגדרים ומאובטחים).
    2. מערכות ורשתות תקשורת ימודרו, והגישה תותר לפי העיקרון "הצורך לדעת".
    3. הגישה לרשתות מחשב ציבוריות "אינטרנט" מותרת תוך הגבלת גישה, לכל עובדי החברה בכל רמות ההיררכיה, לאתרים הבאים בהתאם לקווים שפורום ההנהלה התווה:
       1. מין.
       2. אלימות.
       3. פשע.
       4. סחר מקוון.
       5. הימורים.
       6. שיתוף קבצים.
    4. יישמרו כללי התקשרות קפדניים לגישה מבחוץ אל רשת החברה.
    5. תקוים בקרת LOG שוטפת לאיתור חריגות ממדיניות החברה וקיום אירוע חריג.
    6. תופעל מערכת DLP לאיתור וקבלת התראות לגבי הוצאת מידע חסוי מחוץ לחברה בניגוד לנהלים.
12. מהימנות עובדים:
    1. מהימנות העובדים, יושרם ואמינותם הנם בסיס לחוסנה של “התאחדות לכדורגל” ".
    2. פורום ההנהלה יגדיר את רמת המהימנות הנדרשת מעובדי החברה, לרבות עובדי הממשקים העסקיים, בהתאם לתפקיד המיועד והמקוים.
    3. פורום ההנהלה יגדיר את דרכי הבדיקה ואימות המהימנות הנדרשים מבעלי התפקידים, תוך התייחסות לאמות המידה הנוגעות לרגישות המידע שיחשפו איליו.
13. אבטחת ממשק עסקי:
    1. ב”התאחדות לכדורגל” מועסקים עובדים אשר אינם נמנים על העובדים הקבועים של החברה (ניקיון, כוח עזר, עובדים זמניים וכדומה), גורמים אלה נבדלים זה מזה בהיקף ובאופן חשיפתם למידע המצוי בחברה. חלקם רשאים להיכנס לאזורי עבודה מסוימים אך אמורים להיות מנועים מחשיפה למידע רגיש, בעוד לאחרים הרשאות גישה גורפות לכלל מערכות המידע, הנתונים ואזורי העבודה.
    2. תחת הגדרת "ממשק עסקי" נמנים לקוחות, ספקים חברות בנות ואחרות אשר יש להם גישה למידע ולמערכות התומכות של החברה.
    3. מצב זה מהווה סיכון אבטחתי גדול העלול לגרום לכשלים ולהגעת מידע לגורמים לא מורשים.
    4. פורום ההנהלה יקבע את רמות סיוג המידע אשר יחשפו לממשק העסקי וכן את ההגנות וההתראות הנדרשות.
    5. באחריות מנהל אבטחת המידע לקיים את הבקרות לבדיקת יישום ההנחיות.
14. מידור המידע והרשאות גישה:
    1. יבוצע מידור של המידע ושל המשתמשים בו בהתאם לתפקיד המוגדר.
    2. לכל תפקיד יוגדר פרופיל משתמש בהתאם לעקרון "הצורך לדעת".
    3. יקוים עקרון "הפרדת סמכויות" בין גורמים מפתחים, בודקים ומאשרים, וכן בין גופים ניהוליים.
    4. פרופיל המשתמש (JOB) יגדיר הרשאות גישה פיזיות במתחם החברה וכן למערכות המחשב והמידע האגור בהם.
15. אחריות אישית לאבטחת המידע:
    1. המנהלים בחברה ישאו באחריות כוללת להטמעה ויישום מדיניות אבטחת מידע של החברה והנהלים הנגזרים ממנה.
    2. כל עובד “התאחדות לכדורגל” אחראי לכלל המידע המצוי בחזקתו, לרבות כזה אשר נשלח או הועבר אליו על-ידי גורם אחר מהחברה או מחוצה לה.
    3. כל עובד אחראי לאבטחת המידע בנושאים עליהם הוא מופקד.
    4. אחריות לאבטחת מידע מתייחסת לאבטחה הפיזית, אבטחת הרשומות והאבטחה הלוגית.
    5. הנהלת החברה מצפה מכל עובד לראות עצמו כאחראי ולדווח באופן מיידי לצוות הניהולי על כל אירוע או חשד לאירוע אשר עלול להשפיע על אבטחת המידע של החברה.
16. איסור שינוי בלתי מבוקר:
    1. יוגדרו נהלים המתווים את אופן ביצוע השינויים בנתונים, בטבלאות המערכת, בתוכנות יישומיות ותשתיתיות של החברה.
    2. חל איסור על ביצוע שינוי בנתונים שלא במהלך הפעילות הרגילה, בתוכנה יישומית ותשתיתית ובחומרה, אלא אם הדבר נעשה באופן מאובטח ומבוקר ובהתאם להנחיות בקובץ נהלים זה.
17. בקרת שינויים ותחזוקה שוטפת:
    1. מנהל אבטחת המידע של החברה יהיה מעורב בכל שינוי המפרטים הטכניים של המערכות ברמת החומרה והתוכנה, אשר עשוי לשנות את מצב אבטחת המידע.
    2. בכל מקרה של חוסר וודאות וספק לגבי הצורך במעורבותו של מנהל אבטחת המידע, יש לערב אותו בנושא.
18. גיבויים:
    1. כלל המידע במערכות החברה יגובה וייבדק באופן שוטף.
    2. מנהל מערכות המידע וצוות ה System יגדירו את תהליכי וכלי הגיבוי.
    3. צוות ה system יתפעל ויתחזק את כלי ותהליכי הגיבוי, כנדרש.
    4. מצעי הגיבוי יאוחסנו בכספות חסינות אש בכל עת, והמצעים התקופתיים יאוחסנו מחוץ למתחם החברה.
19. התגוננות מפני תוכנות זדוניות:
    1. פורום ההנהלה לנושא אבטחת מידע יתווה ויגדיר את ההגנות הנדרשות מפני תוכנות זדוניות ופוגעניות ואופן הטיפול בהן.
    2. מנהל אבטחת המידע יגדיר את התהליכים והכלים הנדרשים לעדכון שוטף של תוכנות ההתגוננות התואמות לסיכונים הדינאמיים בשוק ובכפוף לטכנולוגיות העדכניות הקיימות, אשר נועדו לאתר תוכנות זדוניות.
20. הצפנות:
    1. יעשה שימוש במוצרי הצפנה אשר ימנעו חשיפתו של מידע רגיש המצוין בהערכת הסיכונים ובהתאם לנדרש בחוק.
    2. מנהל אבטחת המידע יגדיר את התהליכים והמוצרים הנדרשים התאם לעקרונות שהותוו ע"י הפורום.
    3. באחריות צוות ה System לתחזק, לתפעל ולעדכן בכל עת את כלי ותהליכי ההצפנה.
21. Supplier Relationships יחסי ספק
    1. בקשרים עם ספקים תינתן תשומת לב להבטי אבטחת מידע הנדרשים בקשר בין הצדדים, בכל קשר עם קבלני משנה קיימת התייחסות לא"מ
    2. בעת מיסוד קשרים עם קבלני משנה וגורמי צד ג' אשר עובדים עם ומטעם החברה תינתן תשומת לב להיבטי אבטחת מידע הנגזרים ממהות הקשר בין הצדדים ולקוחות החברה.
    3. גורמי צד ג' הנותנים שירות לחברה יחתמו על הסכמי חיסיון תוך התחייבות לעמידה במדיניות ודרישות אבטחת מידע של החברה, בהתאם לסוג השירות המסופק, באופן שלא תיפגע רמת אבטחת המידע הקיימת בחברה והלקוח.
    4. הרשאות גישה לנציגי הספק / צד ג' יינתנו בהתאם למדיניות בקרת גישה של החברה.
    5. במידה והספק ישמור ברשותו מידע רגיש של החברה או לקוחותיו יעשה הדבר באישור המנכ"ל לאחר שבוצע סקר הערכת סיכונים והוגדרו הבקרות וההגנות הנדרשות.
22. בקרה וכלי בקרה:
    1. פורום ההנהלה יתווה את עקרונות הבקרה, כנגזר מהאיומים והסיכונים שהוגדרו ואותרו בהערכת הסיכונים. עקרונות הבקרה ייושמו בכל חמשת מעגלי אבטחת המידע.
    2. מנהל אבטחת המידע יגדיר את אמצעי ותהליכי הבקרה בנושאי אבטחת המידע של החברה.
    3. מנהל אבטחת מידע ו/או בא כוחו יבקר באופן שוטף ואקראי את הפעילויות המתבצעות במידע ובתהליכים, בכדי לוודא כי החברה עומדת בדרישות החוקים, התקנות, התקנים והנהלים ובהתאם לכללי המינהל התקין.
    4. נציגי ההנהלה יוודאו יישומם של תהליכי וכלי הבקרה, כל אחד בתחום החברה שבאחריותו.
23. נתיב בקורת:
    1. ייושמו כלים המאפשרים זיהוי חד-ערכי של משתמשים אשר ביצעו שינויים במידע או בתוכנה או אשר ניגשו למידע רגיש, תוך פירוט הפעילות שבוצעה וזמן הביצוע, לפי הגדרות מנהל מערכות מידע.
    2. רמת רישום הפעילות:
       1. רמת הרשת – רישום גישה מצד גורמים מרוחקים, ניסיונות חדירה וגישה למערכות רגישות.
       2. רמת האפליקציה – גישה לפעילויות ומידע רגיש על ידי המשתמש. התיעוד יבדיל בין שינוי לקריאת המידע.
24. ניהול המשכיות עסקית BCP:
    1. BCP – Business Continuation Planning - המשכיות עסקית נועדה לסקל הפרעות לפעילותה העסקית של החברה, ולהגן על תהליכים עסקיים רגישים מפני כשלים ואסונות העלולים להתרחש.
    2. פורום ההנהלה יתווה את העקרונות והכלים עליהם תושתת התוכנית.
    3. אסטרטגיית התוכנית תתבסס על הערכת סיכונים ורגישות המידע והתהליכים.
    4. באחריות מנהל אבטחת המידע ונציגי ההנהלה, כל אחד בתחומו, לבקר, לפקח ולאכוף אחר יישום שלבי התוכנית, וכן לקיים תרגילים ועדכונים מידי תקופה.
25. הדרכה והטמעה.
    1. מנהל אבטחת המידע יפעל להעלאת המודעות לאבטחת מידע בקרב החברה והממשקים העסקיים.
    2. הטמעת היבטי אבטחת מידע יכללו את כל מעגלי אבטחת המידע.
26. תוכנית עבודה ותקציב:
    1. מנהל אבטחת המידע יגבש תוכנית שנתית לקיום ומימוש מדיניות הנהלה לנושא אבטחת מידע.
    2. פעילות אבטחת המידע תשולב בתוכנית העבודה השנתית והרב שנתית של החברה ותתוקצב בהתאם.
27. טיפול בחריגים:
    1. מנהל אבטחת המידע יבצע בקרה שוטפת אחר הפעילות במעגלי אבטחת המידע בחברה ובחברות הבנות, לאיתור פעולות חריגות.
    2. יקוים הליך מסודר וידוע לדיווח וטיפול בחריגות ממדיניות החברה.
    3. חריגות והפרות של מדיניות אבטחת המידע המאותרות על-ידי גורמי החברה ידווחו להנהלת החברה להמשך טיפול וחקירה.
    4. חריגה ממדיניות אבטחת המידע של “התאחדות לכדורגל” והנהלים הנגזרים ממנה, מהווה הפרת משמעת אשר תטופל על ידי ההנהלה.
    5. פורום ההנהלה ידון בישיבותיו באירועים החריגים במטרה לקיים הליך של הפקת לקחים, לימוד ושיפור מתמיד.
28. התאמה:
    1. פורום ההנהלה לנושא אבטחת מידע יזהה ויגדיר את החוקים, התקנות והנהלים אשר החברה מחויבת לקיים בהיבט אבטחת מידע.
    2. מנהל אבטחת המידע יקיים מידי תקופה מבדק התאמת מערכת ניהול אבטחת מידע לנדרש בחוקים ובתקנים ואת מידת היישום בשטח.
    3. באחריות מנהל אבטחת המידע לעדכן את מדיניות החברה והנהלים הנגזרים ממנה בהתאם לצורך והחלטות הפורום.
    4. מדיניות ונהלי אבטחת המידע חלים על כל עובדי “התאחדות לכדורגל” לרבות הממשקים העסקיים.