## נוהל תגובה לאירועי 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. כללי:
   1. “התאחדות לכדורגל” (להלן "הארגון") מחזיק מערכות מידע הכוללים מידע חסוי וחסוי ביותר.
   2. ישנה חשיבות רבה לשמירה על המידע, תוך כדי אפשרו תהליכי עבודה תקינים בארגון.
   3. לצורך שמירה על עבודה רצופה, חיסיון ושלמות המידע, יש צורך בזיהוי, דיווח ותגובה מהירה של אירועי אבטחת מידע לגורמים הרלוונטיים בארגון.
   4. במסגרת ההדרכות התקופתיות בנושא מודעות העובדים לענייני אבטחת מידע, ידריך ויעדכן מנהל האיכות והדרכת מערכות באמ''מ את עובדי החברה, לרבות עובדי הממשקים העסקיים בדבר ההליך בנוהל זה.
2. מטרה:
   1. הגדרת התהליך לדיווח וטיפול באירועי אבטחת מידע.
   2. הגדרת מתודולוגיה של תגובה לאירועי אבטחת מידע וכל הגורמים הקשורים בה.
   3. צמצום הנזק שיכול להיגרם כתוצאה מאירועי אבטחת מידע.
   4. חזרה לשגרת עובדה רגילה מהר ככל האפשר.
3. אחריות:
   1. באחריות מנהל אבטחת מידע וסייבר לעדכן נוהל זה לפי מידת הצורך והעניין.
   2. באחריות מחלקת תשתיות לסייע באכיפה של נוהל זה .
4. תפוצה:
   1. כל עובדי הארגון
5. הגדרות:
   1. "אירוע אבטחת מידע" – כל אירוע שיש בו כדי לפגוע בזמינות, סודיות או שלמות של המידע או מערכות המידע המכילות מידע, כולל פעילות מכוונת או לא, אשר גרמה או לא גרמה נזק. להרחבה ראה נספי א' לנוהל זה.
   2. "איום" – מפגע פוטנציאלי אשר עלול לפגוע בנכסי\מערכות המידע של הארגון.
   3. "התקפה" – שורה של צעדים הננקטים על-ידי תוקף בכוונה להשיג מטרה שלא אושרה.
   4. "נקודות תורפה" – סוג של כשל בנכס מידע, במערכת או באמצעי הבקרה של המערכת, העלולה להיות מנוצלת ע"י איום. נקודות תורפה יכולה להיחשב גם כ"חשיפה" או "מידת החשיפה" לאיום כלשהו.
   5. "חיסיון" – הבטחת נגישותו של מידע רק לגורמים מורשים.
   6. "שלמות" – שמירת הדיוק והכלילות של המידע ושל שיטות העיבוד.
   7. "זמינות" – הבטחה שמשתמשים מורשים יוכלו לגשת למידע ולמשאבי המחשוב, לפי הצורך.
6. גוף הנוהל:
   1. תהליך דיווח על זיהוי אירועי אבטחת מידע ונקודות תורפה
      1. דרכי גילוי וזיהוי של אירועי אבטחת מידע ונקודות תורפה
         1. אירועי אבטחת מידע וזיהוי נקודות תורפה ניתנים לגילוי בכמה דרכים:
            1. ע"י משתמש או מנהל מערכת, שמבחין באי-סדירות או התנהגות מחשידה בסביבת העבודה שלו.
            2. ע"י התרעות המיוצרות ע"י מערכת המידע (אזהרות מערכת או הודעות שגיאה)
            3. ע"י מרכז ניהול והתרעות אירועי אבטחה ( SIEM / SOC)
            4. ע"י שימוש בכלים ייעודיים לאבחון וזיהוי נקודות תורפה
            5. דרך הודעות ועדכונים חיצוניים, כגון גופי CERT וספקי תוכנה\פתרונות.
            6. ע"י התרעות אשא נאספות ע"י צוות אבטחת מידע (דרך מערכות SIEM או מרכזי SOC)
      2. תפקידים ואחריות בניהול ותגובה לאירועי אבטחת מידע
         1. לצורך תגובה יעילה במקרה של אירוע אבטחת מידע, וניהול האירוע בצורה יעילה במטרה למזער את מידת ההשפעה של האירוע, ו\או הנזק על הארגון, יוגדר צוות תגובה לאירועי אבטחת מידע אשר יגובש מנציגים שיוקצו לכך:
            1. מנהל צוות אבטחת מידע (בד"כ מנהל אבטחת המידע או ממונה על אבטחת המידע)
            2. נציג צוות סיסטם, תקשורת ואבטחת מידע
            3. מנהל בסיסי נתונים- DBA (לפי הצורך)
            4. נציג מאגף הביטחון (לפי הצורך)
            5. נציג ממחלקה משפטית (לפי הצורך)
            6. נציג ממחלקת משאבי אנוש (לפי הצורך)
         2. על מנהל אבטחת מידע באמ''מ לדאוג לרשימה מעודכנת של כל נציגי הצוותים (ראה נספח ו' לנוהל זה) ודרכי התקשורת איתם ולעדכן את הרשימה אחת לחודש או בעת הצורך.
         3. לצוות התגובה תוקצה כתובת דוא"ל ייחודית (ראה נספח ו' לנוהל זה) שדרכה יועברו הדיווחים הרלוונטיים. לכל חברי הצוות תהיה גישת קריאה לתיבה ולמנהל הצוות יהיו הרשאות ניהול על התיבה.
         4. לאחר קבלת מידע על האירוע (הגדרת סוג האירוע ודרכי הדיווח מוגדרים במסמך מדיניות ניהול אירועי אבטחת מידע) יעודכן מנהל צוות התגובה לאירוע ומאותו רגע ואילך הוא יוגדר כמנהל האירוע.
         5. תפקידו של מנהל האירוע הוא לקבוע את סדר הפעולות לטיפול באירוע לפי אופי וסוג האירוע, לחלק אחריות לביצוע של משימות ולקבוע לו"ז לדיווחי סטאטוס וביצוע.
      3. חובת הדיווח של משתמש על אירועי אבטחת מידע ונקודות תורפה
         1. על כל עובד בארגון (פנימי או חיצוני) לדווח על כל פעילות חשודה בסביבת העבודה שלהם למוקד התמיכה במיידית.
         2. כל עובד באגף מערכות מידע, לרבות צוות הסיסטם (System) ידווחו ישירות לצוות תגובה לאבטחת מידע על כל זיהוי של אירוע אבטחה במערכותיהם על סמך ניסיונם והיכרותם עם המערכות.
      4. תהליך הדיווח על אירוע אבטחת מידע וזיהוי נקודות תורפה
         1. באחריות כל עובדי הארגון (פנימיים וחיצוניים כאחד) לדווח מיידית על כל אירוע אבטחת מידע.
         2. משתמשי הקצה ידווחו לנציג התמיכה הטכנית על כל אירוע אבטחת מידע.
         3. נציג התמיכה יערוך ניתוח ראשוני של האירוע.
         4. באחריות נציג התמיכה לפתוח דו"ח תקלה רגיל ומדויק עם כל פרטי האירוע כולל פרטים נוספים שנציג תמיכה טכנית חושב שהם רלוונטיים לניתוח המקרה (כולל צעדים שיינקטו או ננקטו) – כפי שמפורט בדו"ח דיווח אירוע אבטחת מידע (ראה נספח ה' לנוהל זה).
         5. נציג תמיכה טכנית יעביר את הטיפול באירוע לצוות אבטחת מידע, במידה וההבנה הראשונית שלו אכן מצביעה כי זהו אירוע אבטחתי.
         6. מנהלי מערכות ידווחו ישירות לצוות אבטחת המידע דיווח כוללני שמכיל בתוכו פרטים על המערכות, מיקומן ברשת והמהלכים שהובילו את איש צוות הסיסטם (System) להבין כי מדובר באירוע אבטחתי.
         7. מנהלי צוות אבטחת מידע יודיעו לחברים הרלוונטיים בצוות אבטחת מידע על אירוע אבטחה ויחיל במקביל במתן מענה לאירוע על מנת לסיימו מהר ככל האפשר ולחזור לשגרת עבודה תקינה.
         8. הדיווח הראשוני תמיד ייעשה בטלפון, על מנת להבטיח תגובה מהירה מכל הגורמים הרלוונטיים.
   2. תהליך תגובה לאירוע (Incident Response)
      1. כללי
         1. הטיפול באירוע ייקבע עפ"י אופיו וחומרתו, אך יש לעקוב אחר התבנית הבסיסית הבאה בכל טיפול באירוע, כאשר לכל שלב יבוצע תיעוד מלא על-מנת להפיק לקחים להבא.
      2. תגובה מיידית
         1. פעולות שיש לבצען מיידית על-מנת לצמצם את הנזק שהאירוע עלול לגרום ע"י בידוד המערכות שנפגעו.
      3. כינוס צוות התגובה
         1. בשלב זה ייאסף מידע רב ככל האפשר אודות האירוע ממשתמשים ומערכות וגם מגורמים חיצוניים (כגון האינטרנט, ספקי שירותי מודיעין סייבר, גופי CERT, ועוד).
      4. ניתוח האירוע
         1. לאחר איסוף המידע, באחריות מנהל אבטחת מידע לכנס את חברי צוות התגובה הרלוונטיים ולבצע את סדר הפעולות הבא:
         2. ניתוח האירוע
            1. מנהל הצוות יציג בפני חברי צוות התגובה את כל המידע שנאסף וביחד יגזרו משמעויות בנוגע למערכות פגיעות, פוטנציאל הנזק וחומרתו, מצבו הנוכחי של האירוע ואופי ההתפשטות של המפגע.
         3. תוכנית תגובה
            1. לאחר ניתוח הנתונים תבנה תוכנית תגובה לכל אחד מהגורמים הרלוונטיים כולל לו"ז לביצוע. יש לשים דגש על נקודות ממשק בעייתיות בין שני גורמים ומציאת פתרון הולם על מנת לא ליצור עיכובים מיותרים במתן המענה לאירוע.
         4. תגובה לאירוע
            1. מתן המענה של הגורמים הרלוונטיים לאירוע האבטחה. באחריות מנהל אבטחת המידע לעקוב אחר הצעדים שננקטו ולוודא כל צעד גם לצורך מעקב על התקדמות הטיפול וגם לצורך הפקת המסקנות מן האירוע.
         5. הסקת מסקנות
            1. לאחר סיום האירוע, על צוות אבטחת המידע להפיק את המסקנות הנדרשות מן האירוע, דרכי טיפולו על מנת לזהות את הפרצות והליקויים אשר אפשרו את התפתחותו על מנת למנוע הישנות במקרה דומה בעתיד וגם לייצר דרכי עבודה יעילות יותר על סמך העבודה שנעשתה בזמן האירוע בכדי שלהבא הטיפול יהיה טוב ומהיר יותר. על מנהל אבטחת המידע להוציא דו"ח עם כל המסקנות שהופקו, להפיצו לגורמים הרלוונטיים ולתייקו על מנת שישמש בעתיד כמקור התייחסות.
         6. הטמעת צעדי מנע, ניטור ובקרה
            1. בשלב זה יבוצעו צעדים על מנת למנוע תקלות במקרה דומה בעתיד, אשר כוללים:

התקנה של עדכוני תוכנה רלוונטיים בכלל המערכות אשר פגיעות באותה פרצת אבטחת מידע.

ביצוע ריענון של נהלי אבטחת המידע הרלוונטיים.

הקשחת המערכות הפגיעות ו\או ציוד התקשורת\אבטחת מידע.

זיהוי נקודות הכשל והטמעה של אמצעי פיקוח נוספים בנקודות הכשל הספציפיות.

נקיטת פעולות משפטיות כנגד מפגעים חיצוניים ע"י שימוש בראיות שנאספו בזמן האירוע ולאחריו.

נקיטת צעדים משמעתיים כנגד עובדי הארגון ו\או עובדים חיצוניים בתיאום עם הגורמים הרלוונטיים.

ייעשה שימוש בדוחות לפעולות מתקנות ומוענות לצורך מניעת הישנות האירועים.

* 1. תהליך איסוף ראיות
     1. כללי
        1. על מנת לשמור על שלמות וקבילות הראיות, יש צורך לתעד ולוודא את השלמות של הראיות לאורך כל תקופת אחזקת הראיות, מרגע האיסוף, ועד להצגתן בבית המשפט (Chain of Custody).
        2. על הגורם המבצע את איסוף הראיות להיות מוסמך וכשיר לביצוע העבודה, על מנת לא לפגוע ו\או לזהם את הראיות שנאספו.
        3. מרגע איסוף הראיות, יש לאחסן אותם במקום מאובטח, מפני גישה לא מורשית וגרימת נזק סביבתי (חום, לחות, קור, אש, הצפה וכו').
     2. איסוף ראיות פיזיות
        1. יש לאסוף את המדיה\רשומות הפיסיות, ולבצע העתקים, לצורך ניתוח ועבודת התחקור.
        2. אין לעבוד עם המסמכים והרשומות המקוריים.
        3. את המסמכים והרשומות המקוריות יש לאחסן במקום מאובטח (ראה סעיף 6.3.1.3).
     3. איסוף ראיות לוגיות (דיגיטליות)
        1. אין לעבוד ו\או לבצע ניתוח של הממצאים על גבי מדיה המקור שנאספה כראיה.
        2. יש לבצע מספר גיבויים (מהמדיה מקור) ולבצע את כל הניתוח והתחקור הדיגיטלי אך ורק על הגיבויים, ולא על המדיה מקור.
  2. ביקורת על תהליך הפקת לקחים
     1. מנהל אבטחת המידע בארגון יבדוק אחת לרבעון האם יושמו כל הלקחים הנדרשים בעקבות אירועי אבטחת המידע שאירוע באותו רבעון.
     2. אחת לחצי שנה יפיק מנהל אבטחת מידע דו"ח המפרט את כל אירועי אבטחת המידע שהתרחשו במהלך התקופה. הדו"ח יעבור ניתוח מעמיק, על מנת לזהות אירועים חוזרים או אירועים רבי השפעה. הדו"ח יעלה לדיון, אחת לחצי שנה או אחת לשנה במסגרת ישיבת הנהלה (וועדת היגוי לאבטחת מידע).
     3. מנהל אבטחת המידע יבדוק אחת לשנה את עדכניותו של נוהל זה ויהיה אחראי להוסיף נהלים ו\או לבצע שינויים בנהלים הקיימים בהתאם להפקת הלקחים מאירועי אבטחת המידע.
  3. חובת הדיווח למטופלים אשר המידע אודותיהם דלף כתוצאה מאירוע
     1. במקרה של זליגת מידע אודות מטופלים (כתוצאה מאירוע אבטחת מידע) חלה החובה להודיע למטופל.
     2. ההודעה תתבצע בהתאם להנחיות של הנהלת הארגון, ובאישורה בלבד.

נספח א' – דוגמאות לאירועי אבטחת מידע

להלן דוגמאות של אירועי אבטחת מידע ברמה הלוגית (טכנולוגית):

* פרצה למערכות המידע של הארגון,
* גניבת מידע,
* פעילות חשודה בחשבון משתמש,
* חשד לפגיעת קוד עוין – כגון וירוס, השבתת חשבון,
* השבתת מערכת,
* קבצים לא מוכרים על שולחן העבודה,
* הודעות שגיאה לא מוכרות,
* חיבורי רשת לא מוכרים,
* ניסיונות התחברות חשודים ולא מוכרים,
* יישומים חשודים המופיעים פתאום במחשב,
* הודעות על ניסונות חיבור כושלים,
* קבצים פגומים או כל התנהגות חשודה אחרת.

להלן דוגמאות של אירועי אבטחת מידע ברמה הפיזית:

* גניבת ציוד מחשוב (לרבות מחשבים ניידים, טלפונים חכמים, וכל ציוד מחשוב אחר)
* פגיעה פיזית בציוד מחשוב ו\או ארונות תקשורת
* גישה של אדם זר באזור רגיש (ללא ליווי, ו\או ללא תג זיהוי)

להלן דוגמאות של אירועי אבטחת מידע ברמה הניהולית:

* שימוש של משתמש בנתוני גישה של משתמש אחר
* מסירת מידע רגיש לגורם לא מורשה, ע"י עובד הארגון

נספח ב' – דוגמאות לנקודות תורפה

סוג של כשל במערכת או באמצעי הבקרה של המערכת, כגון: תוכנת אנטי-וירוס שלא מעודכנת, מחשב שלא נעול, תיקים אישיים ללא השגחה, אמצעי הזדהות ללא השגחה, חדרים רגישים פתוחים ולא מאוישים, וכדומה .

דוגמאות לנקודות תורפה ברמת אבטחה פיזית וסביבתית:

* מחשבים ניידים "זרוקים" בחדר ללא השגחה.
* דלתות לא נעולות, במשרדים שמחזיקים מידע רגיש
* אמצעי זיהוי (כגון כרטיס חכם) על שולחן העבודה

דוגמאות לנקודות תורפה ברמת אבטחה לוגית (טכנולוגית):

* חשבונות משתמשים המתנהלים ללא סיסמאות.
* סיסמאות חלשות (ברורות מאליהן וקלות לניחוש|) למערכות רגישות
* גישה למאגרי מידע רגישים ללא יישום הרשאות משתמשים

נספח ג' – יומן אירועי אבטחת מידע

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| תאריך האירוע | שעת האירוע | מודיע האירוע | מהות האירוע | מטפל באירוע | סטאטוס |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

\* על כל אירוע, חובה לתעד ולמלא דו"ח אירוע (ראה נספח ד' לנוהל זה).

נספח ד' – דו"ח טיפול באירועי אבטחת מידע

|  |
| --- |
| שלבי עבודה:  מרכז תמיכה יפתח קריאה במערכת הקריאות.  במידה והאירוע חמור (עלול להגיע להשבתה של מערכת קריטית) הנציג תמיכה טכנית ימלא טבלה זו.  לאחר סיום האירוע הדף יימסר למנהל אבטחת המידע בארגון.  מנהל אבטחת המידע יוודא שהאירוע מתועד כראוי, יחתום בתחתית הדף ויתייק אותו בקלסר "יומן טיפול ומעקב באירועי אבטחת מידע" (ראה נספח ג' לנוהל זה). |

|  |  |
| --- | --- |
| שם מקבל הדיווח הראשוני: |  |
| מספר קריאה: |  |
| תאריך: |  |
| שעת הדיווח הראשוני: |  |
| מקור הדיווח הראשוני: |  |
| אתר\מיקום המדווח ו\או האירוע: |  |
|  | |
| תיאור האירוע |  |
| תיאור המקרה |  |
| פרטים ראשוניים נמסרו ל: |  |
| שם האחראי לטיפול באירוע: |  |
| הטיפול באירוע: |  |
| תוצאות הפגיעה: |  |
| תאריך סגירת האירוע: |  |
| שעת סגירת האירוע: |  |
| סיכום ומסקנות האירוע (כולל הפקת לקחים והמלצות) |  |
| תיעוד: |  |
| מס. דפ"מ (ISO 27001): |  |

תאריך:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

שם ממלא הדו"ח: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

חתימת מנהל תחום אבטחת מידע: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

נספח ה' – הנחיות לטיפול ותגובה לאירועי אבטחת מידע שונים

טיפול במתקפת וירוסים

1. אם יש חשד לווירוס במערכת כלשהי, על המשתמש לנתק מיד את המחשב מהרשת ולפתוח קריאה במרכז תמיכה על אירוע אבטחת מידע.
2. רק באישור מנהל המחשוב ו\או מנהל אבטחת המידע יחובר המחשב אל הרשת מחדש.
3. חברי צוות הסיסטם ותקשורת יפעלו יחד לאתר את מקור ההדבקה בווירוס ולבדוק האם נדבקו מחשבים נוספים בארגון על מנת להבטיח מתן מענה מלא לבעיה ומניעת הדבקה חוזרת ונשנית של מחשבים בארגון.
4. מנהל אבטחת המידע ינהל את האירוע.
5. מנהל אבטחת המידע ישקול לבודד את האתר הנפגע על מנת למנוע התפשטות הווירוס לאתרים נוספים ברשת הארגונית.

נספח ו' – צוות תגובה לאירועי אבטחת מידע

להלן צוות התגובה לאירועי אבטחת מידע בארגון:

* מנהל אבטחת מידע
* מנהל מחשוב
* מנהל תשתיות
* מנהל\אחראי בסיסי נתונים (DBA)
* נציג מצוות פיתוח