## נוהל מדיניות הצפנה

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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: 01.01.2019 | תאריך תיקוף המסמך: | | סטאטוס המסמך: סופי | |   טבלת שינויים   |  |  |  |  |  | | --- | --- | --- | --- | --- | | תאריך שינוי | מהות השינוי | סעיפי השינוי | גרסה | גורם מאשר | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |

1. רקע:
   1. “התאחדות לכדורגל” (להלן "הארגון") מנהל ומחזיק מידע רב הכולל גם מספר מאגרי מידע רשומים, הכוללים פרטים אישיים על העובדים. כדי למנוע פגיעה בחיסיון, לשמור על שלמות וזמינות המידע, ולמנוע חשיפת מידע העשוי לפגוע בפעילות של הארגון, נדרש להפעיל שירותי הצפנה שונים על השימוש במידע.
   2. מסמך זה בא למסד עקרונות מנחים לשימוש בשירותי הצפנה.
2. מטרות:
   1. להגדיר קווים מנחים אודות שימוש בשירותי ההצפנה במשרד.
3. אחראי לביצוע הנוהל:
   1. צוות תשתיות – אחריות ביצוע.
   2. מנהל אבטחת מידע – אחריות פיקוח.
4. מסמכים ישימים:
   1. מדיניות אבטחת מידע של הארגון.
   2. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
5. הגדרות ומונחים:
   1. "*הצפנה*" – תהליך מתמטי של קידוד נתונים לצורה בלתי קריאה.
   2. "*הצפנה סימטרית*" – מפתח סימטרי, המשותף מראש, מבין שני צדדים אשר רוצים להעביר ביניהם מידע בצורה מאובטחת.
   3. "*הצפנה אסימטרית*" – שיטת הצפנה שבה נעשה שימוש בזוג מפתחות (מפתח פרטי ומפתח ציבורי).
   4. "*PKI*" – תשתית טכנולוגית שמבוססת על תהליכי הצפנה אסימטריים.
6. גוף המסמך:
   1. הנחיות כלליות
      1. על כלל המשתמשים חלה החובה להגן על סודיות המידע שמוגדר במשרד כרגיש, ועליהם לפנות את מסמכי מדיניות ונהלי המשרד בנושאי שימוש בשירותי הצפנה, לקבלת הנחיות מתאימות.
      2. כל מידע שיוגדר כרגיש מחויב בהצפנה, בין בתנועה לרבות בשלבי העיבוד השונים ובין במנוחה, לרבות מחוץ לארגון.
      3. התקנים ניידים, ביניהם מחשבים ניידים, מכשירים סלולריים, מחשבי לוח וכדומה, נדרשים בהצפנת רכיבי האחסון בהם.
      4. על ההצפנה להתבצע הן ברמת תשתית והן ברמת האפליקציה (במידת האפשר).
   2. תקשורת במעבר
      1. נתונים במעבר נפוצים בשתי קטגוריות עיקריות
         1. מידע ציבורי לא מאובטח ברשתות פתוחות, כגון אינטרנט
         2. נתונים ברשתות פרטיות, כגון רשת תקשורת פנימית בארגון
      2. מידע העובר ברשתות פתוחות ופנימיות, צריכים להיות מוצפנים באחת מהאפשרויות הבאות:

|  |  |  |
| --- | --- | --- |
| דרישה עסקית | שיטת הצפנה | אלגוריתם |
| חיבור רשתות פרטיות על גבי רשת מהימנה | Virtual Private Network (VPN) | לפחות 3des |
| אבטחת אתרי אינטרנט ציבוריים על גבי רשת לא מהימנה | Transport Layer Security (TLS)  Secure Socket Layer (SSL) | לפחות TLS1.1 |
| אבטחת רשת על גבי רשת מהימנה | Transport Layer Security (TLS)  Secure Socket Layer (SSL) | לפחות TLS1.1 |

* + 1. Transport Layer Security (TLS) הוא הפרוטוקול המומלץ לאבטחת אתרי אינטרנט ושירותים על גבי רשתות מהימנות בשל פרצות מוכרות ב Secure Socket Layer (SSL)
  1. מידע ברשת הארגון
     1. מידע ברשת הארגון, הוא מידע הנמצא על גבי מחשבים שולחניים וניידים, ועל גבי שרתים. כמו כן המידע נמצא בקבצי log קבצי יישומים, קבצי תצורה ובמקומות נוספים.
     2. כדי להגן על מידע ברשת הארגון, הצפנת בסיס הנתונים נדרשת כדי להגן על המידע.
     3. נדרשת הצפנה כדי להגן מידע רגיש בארגון (Column/Cell-level encryption)
     4. נתונים בארגון צריכים להיות מוגנים באחת מהאפשריות הבאות:

|  |  |  |
| --- | --- | --- |
| שיטה | שיטת הצפנה | אלגוריתם |
| אחסון (Storage level) |  |  |
| דיסק מלא (Full disk) |  |  |
| קובץ / ספריה (File/Folder) |  |  |
| בסיס נתונים (Full database) |  |  |
| Column/Cell-level |  |  |

* 1. ניהול מפתחות ההצפנה
     1. כללי
        1. דרישות אבטחת מידע בנושא מפתחות, אורך, שיטות וטכנולוגיה יעודכנו מעת לעת בהתאם להתפתחויות הטכנולוגיות ובכל מקרה לא יעשה שימוש בטכנולוגיות מיושנות ו\או הידועות כפריצות.
        2. ככלל, כל מפתחות ההצפנה יוחלפו אחת לשנה (במידת הישימות).
     2. תהליך יצירת מפתחות
        1. יש לקבוע תהליך מוסדר של יצירת מפתחות הצפנה עבור כל שירותי ההצפנה אשר בשימוש המשרד.
        2. תהליך יצירת המפתחות יתבצע אך ורק ע"י גורמים מורשים לכך.
        3. השימוש בשירותי הצפנה יתבצע בהתאם להנחיות מסמך זה:
           1. הצפנה סימטרית – אורך מפתח מינימאלי יהיה 256 ביט.
           2. הצפנה אסימטרית – אורך מפתח מינימאלי יהיה 2048 ביט.
        4. ככלל, תוקף התעודה ו\או מפתח יהיה עד שלוש שנים לכל היותר.
     3. בעל המפתחות (Key Ownership)
        1. כל מפתחות ההצפנה צריכים להיות משויכים לגורם אחראי אחד, אשר יהווה כבעל המפתח, והוא יהיה אחראי על כל מחזור החיים של המפתח.
        2. יש לתעד (ברשימה) את כל בעלי מפתחות ההצפנה אשר נמצאים בארגון.
     4. תהליך הפצת מפתחות ההצפנה
        1. תהליך הצפת מפתחות ההצפנה יתבצע בצורה מאובטחת, כך שימנע גישה מגורמים שאינם מורשים לכך.
        2. במידת הישימות, תהליך הפצת מפתחות ההצפנה יתבצע באופן ידני, על מנת למנוע גישה לא מורשית למפתחות ההצפנה.
        3. אין להפיץ את מפתחות ההצפנה באמצעות הדוא"ל, או כל תעבורה שאינה מאובטחת כלל.
     5. שמירה על מפתח הצפנה
        1. מפתח הצפנה הישמר בכספת או בספריה עם סיסמה, כדי למנוע גישה לא מורשית לקובץ
     6. ביטול במפתח הצפנה
        1. ביטול מפתח הצפנה לפני שהוא פג תוקף
        2. מפתח הצפנה ייבוטל כאשר יש חשש כי הוא נפגע, או אין צורך בשימושו
     7. שחזור מפתח הצפנה
        1. תהליך שחזור מפתח הצפנה חייב להבטיח כי רק גורמים מורשים ייקבלו את מפתח ההצפנה
        2. בבקשה לשחזור מפתח הצפנה חייבים לזהות את מבקש השחזור ולוודא כי הוא מורשה לקבל את מפתח ההצפנה
     8. פגיעה במפתח הצפנה
        1. במקרה שמפתח הצפנה נפגע, יש לדווח למנהל התשתיות ולמנהל אבטחת מידע ולבעל המידע שמפתח ההצפנה מקושר אליו
        2. מפתח ההצפנה יוחלף / יושמד. מפתח הצפנה חדש יוגדר
        3. המידע שנחשף / נפגע יוצפן על פי מפתח ההצפנה החדש
     9. חידוש מפתח הצפנה
        1. תהליך חידוש מפתח הצפנה ייעשה בהתאם לתהליך יצירת מפתח הצפנה
        2. חידוש מפתח הצפנה ייעשה במקרים הבאים:
           1. לא נעשה שימוש לרעה במפתח הצפנה ואין חשש כי מפתח ההצפנה נפגע
           2. עברה שנה מעת יצירת מפתח ההצפנה
     10. ביטול מפתח הצפנה
         1. מפתח הצפנה יהיה שימוש מוגדר (כדוגמא: דואר אלקטרוני, הצפנת מידע, חתימה אלקטרונית, הצפנת מידע בתעבורה)
     11. השמדת מפתח הצפנה
         1. השמדת מפתח הצפנה תהיה לצמיתות בכל הארכיון של גיבוי, בכל המערכות ואמצעי תקשורת
         2. השמדת מפתח חייבת להבטיח כי כל העקבות של מפתח הצפנה יוסרו ללא אפשרות שחזור
         3. מפתח הצפנה יושמד כאשר אין צורך בשימושו
  2. דרישות חוקיות ורגולטוריות לשימוש בשירותי הצפנה
     1. השימוש בשירותי הצפנה ברשת המשרד יתבצע בהתאם למקובל בחוק ורגולציות רלוונטיות לארגון.
     2. על מנהל אבטחת המידע להתעדכן אל מול המחלקה המשפטית בגין דרישות חוק ורגולציה מקומית ובינלאומיות (במידת הישימות) לשימוש בשירותי ההצפנה, ולוודא תאימות לדרישות הללו.
  3. אכיפה
     1. יש לשמור על ההנחיות המוגדרות במסמך מדיניות זה.
     2. כל חריגה ממדיניות זו מחייבת קבלת אישור (בכתב) ממנהל אבטחת המידע במשרד.
        1. כל הפרה ממדיניות זו, עלולה להוביל לנקיטת אמצעים משמעתיים.