## נוהל מדיה נתיקה

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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. “התאחדות לכדורגל” (להלן "הארגון") מפעיל מספר מערכות מידע, אשר מכילות בין היתר מידע רגיש.
	2. הארגון עובד באופן שוטף ולפי הצורך עם מידע המכיל פרטים רגישים הכוללים מידע על : בתי עסק, תאגידים, לקוחות, אזרחים, בנקים וכד'. המידע נשמר בקבצים במדיה אלקטרונית או על נייר. מידע זה רגיש בחלקו ובמידה וייפול לידיים לא מורשות או ימחק בטעות או בזדון עלול להיגרם נזק לארגון, ללקוחות או לצד ג' כלשהו.
	3. כלל כחלק מהנחיות לעובדים חל איסור לחבר או להכניס כל מדיה מגנטית פרטית או של גורם חיצוני למחשבי הארגון (דיסק און קיי, CD, DVD, דיסק קשיח חיצוני, וכו').
	4. עם זאת לעיתים קרובות יש צורך לבצע שימוש באמצעים נתיקים למשתמשי המחשב בארגון אשר נזקקים לבצע העברת נתונים פנימה או החוצה מחוץ למערכות המחשוב. פעילות מסוג זה עשויה לחשוף את הארגון לסיכונים שונים, אשר עלולים לפגוע ביציבות המערכות או סודיות המידע.
2. הגדרות
	1. USB Flash Drive– אמצעי נתיק בעל זיכרון אשר באמצעותו ניתן לשמור מידע והוא מתחבר למחשבי הארגון באמצעיות חיבור USB
3. מטרה:
	1. הגדרת אופן פעולה בנושא חיבור אמצעים נתיקים למערכות המחשוב בארגון
	2. מנגנוני הגנה הארגון לבקרה וחסימה אשר תאכוף איסור שימוש במצעי זיכרון נתיקים (כגון דיסקים, זיכרון Flash) ובכל מקרה יוגדר שימוש מותר ואסור תוך התחשבות בצרכי אבטחת מידע.
	3. אופן הטיפול והאבטחה של מצעי זיכרון נתיקים אשר ייגזר בהתאם לשימוש בהם ובמידע האגור בהם
	4. קביעת תהליך מסודר של השמדת מצעים האוגרים מידע רגיש של הארגון.
4. אחראי לביצוע\בקרה הנוהל:
	1. בקרה - מנהל אבטחת מידע והסייבר.
	2. האחריות לסיווג המידע המגובה היא בידי בעל המידע בתאום עם ממונה על מערכות הגיבוי בארגון.
	3. אחריות על שמירה וארכוב הנתונים חלה על מנהל מערכות מידע וממונה מטעמו לנושא זה.
5. מסמכים ישימים:
	1. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
6. גוף הנוהל:
7. 1. מנגנון הגנה למניעת חיבור USB FLASH
	2. על מנת למנוע חיבור עיון או בשוגג לאמצעים נתיקים תופעל מערכת אכיפה ייעודית אשר תבצע את הפעלות הבאות :
		1. המערכת תבצעה חסימה לחיבור USB FLASH לא מאושר
		2. המערכת תוציא אתראה למנהלים רלוונטיים על ניסיון חיבור לא מאושר
		3. המערכת תאפשר ניהול רשימה של USB FLASH מאושרים לחיבור
8. אכיפה
	1. יש לשמור על ההנחיות המוגדרות במסמך מדיניות זה.
	2. כל חריגה ממדיניות זו מחייבת קבלת אישור (בכתב) ממנהל תחום אבטחת המידע במשרד.
	3. כל הפרה ממדיניות זו, עלולה להוביל לנקיטת אמצעים משמעתיים.
9. ביקורת
	1. ביקורת כי על עמדות הקצה הקיימות ושרתים כי קיימים תתבצע ע"י מערכות ייעודיות המנוהלות ע"י מנהל אבטחת מידע.
	2. אחת ל- 6 חודשים, ייזום מנהל אבטחת המידע מהלך לבדיקת תקפות הרשאות המשתמשים לחיבור אמצעים נתיקים .