## נוהל שמירה וטיפול בלוגים

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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. תקשורת לא מאובטחת או מאושרת עלולות לגרום לנזקים חמורים לארגון, כגון: חשיפת מידע רגיש, העברת מידע לגורמים לא מורשים, שינוי לא מורשה של מידע, האטה של הפעילות ברשת ו\או של המחשב הנגוע, מחיקת מידע לא מורשית והשבתה מוחלטת של מערכות המחשוב ב”התאחדות לכדורגל” (להלן "הארגון").
	3. קיימת חשיבות ראשונה במעלה למנוע פגיעה במערך המחשוב בכלל וע"י במערכות הלוגים אשר מתעדות את המידע במערכות
	4. לצורך עבודה שוטפת, יש צורך בהגדרת עקרונות מנחים לניהול ועדכון מערכות לוגים ושמירתם
2. מטרה:
	1. להגדיר תהליכי עבודה בהתקנה, ניהול ועדכון מערכות לוגים
	2. להגדיר את סוג רישום הלוגים, רישומם, מיקום האחסון המתאים, הצפנה והשמדת הלוגים הכרחית להמשך התאמת הארגון לתקנות הגנת הפרטיות
3. אחראי לביצוע\בקרה הנוהל:
	1. בקרה - מנהל אבטחת מידע והסייבר.
	2. ביצוע - מחלקת תשתיות.
4. מסמכים ישימים:
	1. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
5. הגדרות:
	1. מערכת לוגים מרכזית – מערכת אשר מבצעת איסוף לוגים מכל המערכות הרלוונטיות בארגון לנושא כגון מערכות פיירוול , מערכת אנטי וירוס , מערכות הראשות ואפליקציות
6. גוף הנוהל:
	1. תהליך העבודה / שיטת העבודה
	2. תהליך השמירה והטיפול בלוגים הוא הכרחי ונדרש על מנת לשחזר אם ישנו הצורך בעקבות אירוע כזה או אחר שקרה ברשת הארגון . לפיכך, סביבה מאובטחת עבור שמירת הלוגים היא הכרחית.
		1. את האירועים הבאים יש לשמור בתור לוג :
			1. גישת משתמשים אל מידע הארגוני
			2. שעה ותאריך האירוע.
			3. סוג האירוע.( קריאה , כתיבה , עדכון )
			4. גישת אדמין אל כל מערכת המכילה מידע השייך מאגרי המידע הרשומים או המוחזקים
			5. כל ניסיון התחברות (גם שהצליחו וגם כאלו שנכשלו).
			6. שינויי הגדרות, גישה ושינוי קבצי לוג.
	3. על כל הלוגים להיות מטופלים ומאוחסנים.
		1. הנ''ל יעשה באופן הבא :
			1. הגבלת הגישה אל הלוגים על ידי בעלי הרשאות בלבד.
			2. כל מערכות אשר נמצאת ברשימת המערכות המטפלות במידע השייך למאגרי המידע הרשומים או המוחזקים חייבת בלוג
			3. מערכות אבטחת מידע אשר מגינות על מאגרי המידע
			4. הלוגים יישמרו לפחות שנה במערכת.
			5. הארגון יאלץ לבצע ביקורות על מנת לוודא כי אכן קיימים הלוגים על פי הדרישות.
			6. על הארגון לסקור את הלוגים על בסיס יומי.
7. אכיפה
	1. כל עובד שימצא כי הפר את מדיניות זו עשוי להיענש על ידי הגורם הרלוונטי ב”התאחדות לכדורגל”, המחלקה או “התאחדות לכדורגל” עצמו.
8. תחולה
	1. המדיניות חלה על כלל עובדי “התאחדות לכדורגל” (ספקים, עובדי קבלן, יועצים, זמניים) ועובדים אחרים המחזיקים או מתחזקים מידע כלשהו של “התאחדות לכדורגל”.
	2. נוהל זה נכנס לתוקפו מיום פרסומו.
	3. מכניסתו לתוקף, נוהל זה מחליף כל נוהל קודם בעניין.