## נוהל אבטחת פיזית

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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. גישה 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 מערוכת ההגנה פיזית בפרט.
   4. לצורך עבודה שוטפת, יש צורך בהגדרת עקרונות מנחים לניהול הגנה פיזית על מערכות המידע בארגון
2. מטרה:
   1. מדיניות זו מדגישה את המגבלות הפיזיות הנדרשות על מנת להגן על המידע, המבנה ב”התאחדות לכדורגל”.
3. מסמכים ישימים:
   1. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
4. אחריות ביצוע | אחריות בקרה
   1. אחריות ביצוע

כל בעלי המידע ב”התאחדות לכדורגל”.

* 1. אחריות בקרה

מנהל אבטחת מידע

1. תהליך העבודה / שיטת העבודה
   1. כל הציוד המחשוב ב”התאחדות לכדורגל” המעורב במאגרי מידע חייב להישמר בסביבה מאובטחת. רק אנשים הטכנאיים המעורבים בטיפול מאגרי מידע רשאים לגשת אל חוות השרתים.
   2. חוות השרתים של “התאחדות לכדורגל” חייבת להיות מבוקרת בכניסתה ע''י קודן, או כל מנגנון אבטחה אחר שאושר על ידי הביטחון. הבקרה על הכניסה חייבת להיות מתועדת בצורה כלשהי (ע''י שמירת לוגים, מילוי טופס בכניסה וכו').
   3. אדם אשר נכנס אל חוות השרתים חייב להיות בעל תג זיהוי או להיות מזוהה על ידי גורם הביטחון או על ידי ממונה האחראי על החווה.
   4. על המבקרים בחוות השרתים להחזיק בתג זיהוי כלשהו שניתן על ידי הביטחון ב”התאחדות לכדורגל” (תג מבקר) המבדיל אותם מעובדי “התאחדות לכדורגל”.
   5. יש לאבטח באופן פיזי כל נייר או מדיה אלקטרוני המכיל מידע של הכרטיסים החכמים. ''מסמכי עבודה'' חייבים להיות נעולים במהלך היום, אך בסוף היום יש להחזירם למקום מבטחים כגון, כספת או חדר/ מבנה מאושר מבחינת הביטחון לשמירת ניירת רגישה.
   6. כל המידע הרגיש והמידע על הכרטיסים בפרט חייבים להישמר באופן מאובטח בכל עת. השימוש של מלכודות, מצלמות, בקרות אלקטרוניות מורשים על מנת להגן על המבנה.
   7. סקירה של לוגים ומערכת המצלמות תבוצע פעם בחודש.
2. אכיפה

6.1 כל עובד שימצא כי הפר את מדיניות זו עשוי להיענש על ידי הגורם הרלוונטי ב”התאחדות לכדורגל”, המחלקה או “התאחדות לכדורגל” עצמו.

1. 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.