## נוהל גיבוים

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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. מטרת הגיבוי היא לשמר את המידע אשר נמצא על השרתים באתרים השונים ב”התאחדות לכדורגל” במקרה של מחיקתו ופגיעה בו מכל סיבה שהיא.
   2. הגיבוי מתנהל ע"י שימוש בתוכנה חיצונית.  
      שמירת החומר מתבצעת ע"י העברתו למדיות מגנטיות בעזרת טייפ גיבוי חיצוני מסוגים שונים.
   3. קלטות הגיבוי אמורות להיות מוחלפות מדי חודש על מנת שתהיה אפשרות לשחזר חומר שנעלם גם מספר ימים מוקדם יותר.
2. מטרה:
   1. נוהל זה בא לפרט ולהסביר את נהלי הגיבוי ב”התאחדות לכדורגל”. יש לציין כי ביצוע הגיבויים ובדיקת תוצאותיהם הינם באחריות מנהל תשתיות מחשוב .באחריותם לדאוג שגיבוי יבוצע, תוך כדי שמירה על נוהל גיבויים באופן סדיר .
3. מסמכים ישימים:
   1. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
4. אחראי לביצוע הנוהל:
   1. בקרה – מנהל אבטחת מידע והסייבר.
   2. מנהל התשתיות - אחראי על בקרת ביצוע הפעולות המתוארות בנוהל ועל בקרה מדגמית על שלמות הגיבוי
   3. אחראי גיבוי אתרים - חלה האחריות ליישום הנוהל, כל אחד על פי תפקידו ב”התאחדות לכדורגל”
   4. מנהל תשתיות – אחראי על בקרה מדגמית לאופן שמירת הקלטות והשינוע שלהן.
5. הגדרות
   1. שרת – שרת מחשבים מתאפיין בהפעלת מס' רב של תכניות ותהליכי מחשב במקביל, כל תכנית או תהליך משרתים בדרך כלל שרתים אחרים או משתמשי קצה במחשבים המחוברים לשרת וניגשים אליו באמצעות רשת מחשבים על מנת לבקש מידע או להפעיל יישום על גבי השרת. קיימים מס' רב של סוגי שרתים כגון: שרת קבצים, שרת יישומים, שרת נתונים, שרת דוא"ל, שרת DNS, שרת Proxy, שרת WEB וכדומה. קיימים שני סוגים של שרתים כמפורט:
      1. שרת בתור תוכנה אשר מספקת שירותים לתוכנות אחרות ( ,(Clientsבתצורה של "ארכיטקטורת שרת – לקוח".
      2. שרת כמערכת המחשב עליו פועלות התוכנות.
   2. יישום מחשב/תוכנות יישום – תת מחלקה של תוכנת מחשב אשר מנצל את יכולות המחשב ישירות ובאופן יסודי לביצוע משימות אותן המשתמש מבקש לבצע.
   3. בסיס נתונים – הוא אמצעי המשמש לאחסון מסודר של נתונים במחשב לשם אחזורים ועיבודים.
   4. מאגר מידע – אוסף מסודר של נתונים בתחום מסוים, המאפשר אחזור של נתונים אלו לשם הפקת מידע הנחוץ למשתמש.
   5. רכיבי תשתית – רכיבים המשמשים לתפעול טכנולוגיות המידע בארגון כגון: רכיבי חומרה, תוכנה, תקשורת, תחנות קצה, אבטחת מידע. צוות התשתיות הוא זה שאחראי לדאוג לתמיכת המחשוב לזמינות ותפעולם של הרכיבים.
   6. אנטי – וירוס – אנטי – וירוס היא תכנית אבטחה אותה מתקינים על מחשבים או שרתים , על מנת להגן עליהם מפני הדבקות בנזקה. המושג נזקה הינו מושג כללי וכולל בתוכו מספר סוגים של תוכנות זדוניות כגון: וירוסים, תולעים, סוסים טרויאניים ורוגלות ( תוכנות ריגול).
   7. כלי ניהול – כלי המסייע בניהול ותיעוד של עדכונים לשרתים ותחנות קצה באמצעות תוכנת ניהול.
   8. נתב – רכיב תקשורת מחשבים שנועד לקבוע את נתיב והפצה של חבילות נתונים ברשתות תקשורת נתונים.
   9. מתג - רכיב ברשת מחשבים המחבר בין תחנות שונות ברשת. בין אם תחנות קצה או בין רכיבי רשת אחרים כגון : רכזות.
   10. תשתיות מידע ורשתות תקשורת – רכיבים המאפשרים תעבורה של מידע בתוך רשתות הבנק, לרבות רכיבים אשר מספקים הגנה על רשתות אלו.
   11. מחסן נתונים - בסיס נתונים המשמש מערכות תומכות החלטה. בסיס הנתונים מקבל נתונים ממספר מערכות תפעוליות.
   12. תהליך בקרת שינויים –תהליך בקרת שינויים זהו תהליך שמטרתו לתעד ולנהל את תהליך עדכוני אבטחת מידע התהליך יבוצע על ידי אגף מחשוב ויכלול את הנושאים הבאים כמפורט:
       1. תיעוד דרישה ממנהל הגנת הסייבר ואבטחת המידע.
       2. תיעוד זמנים לביצוע עדכונים במערכות החברה.
       3. ביצוע סבב אישורים להתקנת העדכון לסביבת הייצור ובסביבות רלוונטיות נוספות.
       4. וידוא אפשרות לבצע Roll Back במקרה הצורך.
       5. התקנת העדכונים בסביבת הייצור ובסביבות רלוונטיות נוספות.
6. גוף הנוהל:
   1. גיבוי מידע
      1. כל מערכות המידע בארגון יגובו.
      2. אופן גיבוי המידע יקבע בהתאם לדרישות זמינות המערכת.
      3. עבור כל מערכת מידע, בעל המידע יגדיר את רמת הזמינות הנדרשת.
      4. דרישות הזמינות של כל המערכות ירוכזו אצל מנהל אבטחת המידע ויאושרו ע"י וועדת ההיגוי לאבטחת מידע והנהלת הארגון.
      5. כל יום יבוצע גיבוי מלא למידע.
      6. באתרים בהם מבוצעים גיבויים דיפרנציאליים או אינקרמנטליים, יבוצע בכל מקרה גיבוי מלא לפחות אחת לשבוע.
      7. בכל סיום תהליך הגיבוי, צריך לוודא שתופיע הודעה אוטומטית בדבר הצלחה או כשלון הגיבוי. יש לבדוק את הודעה זו בסוף יום העבודה, לצורך ווידוא תקינות הגיבוי.
      8. בכל סיום תהליך גיבוי, מנהל התשתיות יבדוק את קובץ הדיווח (Log File) על מנת לוודא כי הגיבוי תאם לתוכנית הגיבוי הנדרשת. במידה ולא, עליו לדווח על כך למנהל אבטחת המידע, לטפל בתקלה באותו היום, ולבצע גיבוי מלא ברגע שמתאפשר.
   2. מחזורי הגיבוי
      1. מספר מחזורי גיבוי בכל אתר יהיה כדלהלן:
         1. 5 מחזורים יומיים (7 ימים בשבוע)
         2. 6 מחזורים חודשיים (12 חודשים)
         3. 1 מחזור שנתי (7 שנים אחורה)
      2. במידה ולא ניתן יהיה לעמוד במינימום זה, יש להודיע על כך בכתב למנהל אבטחת המידע עם פירוט הסיבה.
      3. הגיבויים יישמרו במרחק של לפחות 15 מטר מחדר השרתים על מנת להפחית מסיכוי שאירוע שיפגע בחדר המחשב לא יפגע בו בזמן במקום שבו שמור הגיבוי, במקום חסין אש ומים ועם הגנות מפני פריצה.
      4. עותק של הגיבויים יוחזק באתר מרוחק.
      5. עותק הגיבויים אשר יוצא מחוץ לאתר הראשי או ה-DR, יוצפן לפני הוצאתו.
      6. גיבוים יוצפנו בעזרת מפתחות ההצפנה אשר יהיו בהתאם לנוהל מפתחות ההצפנה.
      7. מומלץ שלחדר המחשב והתקשורת יהיה אתר DR וגיבוי מרוחק בהתאם לנוהל המשכיות עסקית.
   3. שחזור
      1. באחריות מנהל התשתיות לבצע, באופן יזום, ניסיונות שחזור מדגמיות אחת לחודש ולתעדם. יש לשחזר לפחות קובץ אחד מכל partition של כל שרת.
7. 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.