## נוהל ארכוב והשמדה

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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. מניעת חשיפת חומר חסוי המאוחסן במצעים המגנטיים. הארגון עלול להיקלע למצב משפטי או להתאוששות מאסון בו יהיה צורך להמציא את המידע המקורי על מנת להגן על אינטרסים של לקוחתה , עובדיה, מוצריה או כל שירות אשר הארגון מספקת. כתוצאה מהנ"ל יש צורך לשמור נתונים מעבר לפעילות השוטפת היומית.
2. מטרה:
   1. מטרת הנוהל להגדיר את אמצעים שיש לנקוט בתהליך שמירת ,ארכוב והשמדה של המידע בהתייחס לסוג המידע ורגישותו.
3. 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.
4. מסמכים ישימים:
   1. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
5. גוף הנוהל:
   1. האמצעים לשמירת נתונים:
      1. שמירת קבצי המידע במדיה אלקטרונית או מודפסת יכולה להיעשות באחת מהדרכים הבאות:
      2. באתר המרכזי (ארגון) :
         1. מערכות גיבוי ייעודיות מאובטחת המאפשרות גישה בזמן אמרת למדיה האלקטרונית כגון ארכיון מסמכים, ארכיון דואר וכו'.
         2. מערכות אחסון (Storage) בטופולוגיות המאפשרות גישה בזמן אמרת למדיה האלקטרונית כגון: ארכיון מסמכים, ארכיון הדואר וכו'.
         3. מדיה מגנטית כגון, CD או דיסקים נתיקים בהתאם לרמת הרגישות של המידע המאוכסן בהם ובהתאם לסיווג המידע (נוהל סיווג מידע), אשר ישמרו בתאר הארגון, מוגדרים ומאושרים ע''י סמנכ"ל מערכות מידע ותפעול ובהתאם לנהלי אבטחת מידע ונהלי תפעול רלוונטיים.
         4. מדיה מודפסת כגון דפים, שוברים או כל נייר בהתאם לרמת הרגישות של המידע המודפס בהתאם לסיווג המידע, אשר ישמרו בקופסאות מסומנות ומקוטלגות באיזור תחזוקה של ארגון.
      3. אתר משני \ גיבוי או צד ג'
         1. מערכות ייעודיות מאובטחות בקווי נל"נ ממחשב למחשב אשר מבצעות הרחקת מידע לאתר הגיבוי או לכל אתר אשר יאושר ע"י סמנכ"ל מערכות מידע ותפעול.
         2. מדיה מודפסת כגון דפים, שוברים או כל נייר בהתאם לרמת הרגישות של המידע המודפסת ובהתאם לנוהל סיווג המידע, אשר ישונעו לאתרים מוגדרים מאושרים על ידי מנכ"ל ואשר נמצאים בחוזה עם ארגון ובהתאם לנהלי אבטחת המידע ונהלי התפעול הרלוונטיים.
         3. מדיה מגנטית כגון קלטות גיבוי, CD או דיסקים נתיקים בהתאם לרמת הרגישות של המידע המאוכסן בהם ובהתאם לנוהל סיווג המידע, אשר ישונעו לאתרים מוגדרים ומאושרים ע"י המנכ"ל ואשר נמצאים בחוזה עם ארגון ובהתאם לנהלי אבטחת המידע ונהלי התפעול הרלוונטיים.
      4. סיווג המידע המועבר:
         1. בכדי לקבוע את אמצעי האבטחה שיש ליישם לגבי שמירת הקובץ, יש לסווג את הקובץ בהתאם לנוהל סיווג המידע בארגון.
         2. סיווג המידע בקובץ יעשה על פי רגישות הנתונים בקובץ (מהות הנתונים הנמצאים בו) ועל פי כמות המידע בקובץ (מספר הרשומות).
         3. כל המידע יסווג לאחת מהאפשרויות המתוארות בנוהל סיווג המידע של ארגון.
         4. במקרים של ספק בקביעות רמת רגישותו של קובץ מסוים, יש להיוועץ עם אגף אבטח מידע ולהעדיף סיווג ברמה הגבוהה ביותר.
      5. מידע רגיש במערכות מבוססות אקסל (Excel):

יש להימנע ככל הניתן משימוש במערכות מבוססות אקסל לניהול מידע רגיש. השימוש בקובץ אקסל לצורך זה טומן בחובו סיכונים רבים כאשר הבולטים שביניהם הם:

* + - 1. היעדר יכולת ניהול גרסאות בצורה מסודרת.
      2. היעדר יכולת מעקב אחר שינויים (זהות מבצע השינוי, עיתוי ומהות השינוי).
      3. חוסר במנגנון הרשאות וחוסר יכולת להגן מפני שינויים כתוצאה מכך.
      4. שימוש בפקודות מאקרו שאינן "חתומות".
      5. חשוב לציין- מערכות אשר מנהלות מידע וניתן להוציא מהן "פלט אקסל" אינן רלוונטיות להנחיה זו כל עוד מערכות המקור נותנות מענה לסעיפים שצוינו.
      6. במקרים בהם נדרשת שמירת מידע רגיש במסגרות טבלאיות יש לשאוף לפתרון של מוצר מדף אשר או שילוב מערכות SQL יכיל ניהול גרסאות, יכולת מעקב ומנגנון הרשאות.
    1. קביעת זמן לשמירת נתוני המידע:

לכל קובץ או קטגוריה של קבצים ונתוני מידע המאוכסנים במסדי נתונים חייבת להיות תקופה המגדירה את אורך חייו, לאחר תום פרק חיים מוגדר יושמד המידע בדרך הולמת.

אורך חיים של מידע נקבע ע "י הפרמטרים הבאים:

* + - 1. קביעת מינימום אורך חיים של המידע על פי החוק הרלוונטי או הרגולציה הדורשת את שמירתו.
      2. קביעת נחיצותו של המידע על פי אמות מידה עסקיות.
      3. קביעה האם מידע זה יהיה נחוץ מעבר לדרישות תפעול או דרישות עסקיות כגון הצגה של מסמכים תומכים בדיון משפטי החל במקרה של סכסוך עסקי, תביעת נזיקין, סכסוך עבודה בין עובד ומעביד, וכן לצורך המשכיות עסקית במקרה של התאוששות מאסון.
      4. אורח חיים של מידע יקבע תמיד לפי המועד הארוך ביותר מבין השלושה.
    1. לכל קובץ או קטגוריה של קבצים ונתוני מידע המאוכסנים במסדי נתונים או בלוגים חייבת להיות תקופה המגדירה את אורך חייו, לאחר תום פרק חיים מוגדר, יושמד המידע בדרך הולמת.
    2. דרכי הטיפול במצעי מידע:
  1. מצעים מגנטיים נתיקים (סרטים, קלטות, דיסקטים וכו'), המכילים חומר מסווג בסיווג גבוה, יהיו מאוחסנים תמיד בארון מתכת עם מנעול תליה או בחדר נעול במנעול צילינדר לכל הפחות.
  2. מצעים מגנטיים מקולקלים, ובכלל זה דיסקים קשיחים, לא יוצאו מתחומי המשרד, אם נכלל בהם חומר מסווג בסיווג גבוה (חסוי). המצעים יועברו אל ממונה אבטחת המידע אשר ידאג להשמדתם. הממונה ינהל פרוטוקול לגבי השמדת המצעים הללו.
  3. דיסקים קשיחים מקולקלים אשר מכילים מידע מסווג, ואשר הוחלט לתקנם, יטופלו בתיאום עם ממונה אבטחת המידע רק לאחר קבלת אישורו המותנה בכך כי הספק \ החברה המתקנת התחייבה בכתב לשמור על סודיות מוחלטת ולנקוט באמצעים שהוכתבו מראש על ידי המשרד. טפסי התחייבות לשמירת סודיות יישמרו אצל הממונה אבטחת מידע.
  4. העברת מידע מחוץ לארגון תעשה אך ורק על מצעים מגנטיים (קלטות או דיסקים) חדשים או מצעים מגנטיים של הגוף המקבל.
  5. כל יחידה \ אגף המוציאה מצעים אל מחוץ לכתליה, תנהל מחברת רישומים. זו תאפשר לנתח בכל עת איזה מידע נמסר, על גבי איזה מצע, למי, מתי, אם המצע עצמו אמור לחזור אל השולח וכן אם אכן חזר אל המשרד. כל זאת בכפוף לחוק הגנת הפרטיות. ברישום תעשה אבחנה בין הוצאת חומר ליחידה \ אגף אחר במשרד, לבין הוצאה אל גורם חיצוני מחוץ למשרד.
     1. כל הדיסקים \ קלטות גיבויים בארגון יסומנו בסימון בולט ובמפורש כרכוש של המשרד. אין להשתמש בדיסקים \ קלטות ללא סימון של ארגון.

1. אכיפה
   1. כל עובד שימצא כי הפר את מדיניות זו עשוי להיענש על ידי הגורם הרלוונטי ב”התאחדות לכדורגל”.
2. 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.