**ביקורת תאימות**

**תקנות הגנת הפרטיות**

**XXX**

**רשות האוכלוסין וההגירה**

**23/01/2019**

**© הודעה בדבר זכויות יוצרים:** אין להעתיק, לשכתב, לצלם או לשלוח מסמך זה או חלקים ממנו מבלי לקבל אישור בכתב מרשות האוכלוסין. המידע המופיע במסמך זה הנו רכושו הבלעדי של רשות האוכלוסין. כל הקורא מסמך זה, כולו או מקצתו, ואינו מורשה לצפות במידע המופיע בו, חשוף לתביעה משפטית. המוצא מסמך זה מתבקש להעבירו לידי חברתרשות האוכלוסין, אגף אבטחת מידע.

### תוכן עניינים

1. תמצית מנהלים 3

1.1. רקע 3

1.2. פרטים כלליים 3

1.3. עיקרי הממצאים 3

1.4. סיכום ומסקנות 5

2. פירוט הממצאים 5

2.1. סעיף 2א ו-2ב: מסמך הגדרות המאגר 5

2.2. סעיף 2ג: בחינה שנתית של כמות המידע הנשמר במאגר 5

2.3. סעיף 3: ממונה על אבטחת מידע 5

2.4. סעיף 4: נוהל אבטחה 5

2.5. סעיף 5א: מיפוי מערכות המאגר 6

2.6. סעיף 5ג ו-5ד:ביצוע סקרי סיכונים ומבדקי חדירה למערכות המאגרים ברמת אבטחה גבוהה 6

2.7. סעיף 6א: אבטחה פיזית וסביבתית 6

2.8. סעיף 7א: אבטחת מידע בניהול כוח אדם 7

2.9. סעיף 7ב: ביצוע הדרכות בנושא פרטיות 7

2.10. סעיף 8: ניהול הרשאות גישה 7

2.11. סעיף 9: זיהוי ואימות 7

2.12. סעיף 10: בקרה ותיעוד גישה 8

2.13. סעיף 11א: תיעוד של אירועי אבטחה 8

2.14. סעיף 12: התקנים ניידים 8

2.15. סעיף 13ב: הפרדה בין מערכות המאגר למערכות מחשוב אחרות 9

2.16. סעיף 13ג: עדכונים שוטפים של מערכות המאגר 9

2.17. סעיף 14: חיבור מאובטח לרשת האינטרנט ובגישה מרחוק למערכות המאגר 9

2.18. סעיף 15: מיקור חוץ 9

2.19. סעיף 16: ביקורות תקופתיות 10

2.20. סעיפים 17 ו-18: שמירת נתוני אבטחה וביצוע גיבוי ושחזור לנתונים 10

2.21. סעיף 19: תיעוד חובות בעל המאגר 10

# תמצית מנהלים

## רקע

במהלך חודש נובמבר 2018 ביצעה חברת 2bsecure סקר אצל לקוחות חיצוניים מטעם רשות האוכלוסין XXX הסקר נעשה בדגש על ביקורת תאימות לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 אשר נכנסו לתוקף במהלך חודש מאי 2018. סקר זה בדק ומצא פערים בעמידתה של הלקוח החיצוני בתקנות אלו.

XX מקבל מידע מרשות האוכלוסין מתוקף פקודת הסטטיסטיקה. פקודה זו מאפשרת לXXX לקבל מידע, לעבד אותו ולשמור אותו. הXXX מקבל מידע מ-150 מקורות מידע, כאשר מידע ממרשם האוכלוסין הוא אחד מהם.

## פרטים כלליים

* הXXX מעסיק כ-1,200 עובדים אשר מתוכם כ-800 עובדים מועסקים במשרה מלאה ו-400 נוספים מועסקים כסוקרים טלפוניים / עובדי שטח במשרה חלקית.
* בXXX יש יחידת מחשוב IT הכוללת 130 אנשים. ביניהם עובדים פנימיים ועובדי בתי תוכנה המועסקים שנים רבות. העובדים ביחידת המחשוב הינם: עובדי פיתוח, DBA, פיתוח BI ואנשי תשתיות וסיסטם.
* הXXX מוגדר כבעל מאגר על וכתשתית מידע קריטית ומדווחים למערך הסייבר ברמה שבועית. נוסף לכך, הגוף מונחה יה"ב.
* לXXX יש שני מאגרים רשומים במשרד להגנת הפרטיות: המאגר הסטטיסטי ומאגר העובדים.
* כלל המאגר יושב על רשת עצמאית אשר הגישה אליה היא באמצעות כספות.
* בימים אלו הגוף מלווה על ידי חברת ייעוץ חיצוני להסמכה לתקן 27001.

## עיקרי הממצאים

* נושאים שנמצאו תקינים:
* נהלי אבטחת המאגרים
* אבטחה פיזית
* נושאי גיוס משאבי אנוש
* הפרדת המערכת
* הגבת מודעות
* פערים:
* תיעוד אירועי אבטחת מידע
* בקרה ותיעוד גישה
* שמירה ושחזור נתוני אבטחה
* להלן מפת חום המצביעה על עמידת הלשכה המרכזית לסטטיסטיקה בתקנות בהתייחסות לרמת בקרות כללית לטכנולוגיה ותהליכי עבודה כלליים בלשכה המרכזית לסטטיסטיקה. הפירוט הינו לפי רמת התאימות לסעיפים השונים בתקנות.

|  |  |  |
| --- | --- | --- |
| פרק | נושא  | סטאטוס  |
| 11 | תיעוד של אירועי אבטחה  | אין התאמה |
| 8 | ניהול הרשאות גישה  | התאמה חלקית |
| 10 | בקרה ותיעוד גישה | התאמה חלקית |
| 12 | התקנים ניידים  | התאמה חלקית |
| 17 | שמירת נתוני אבטחה  | התאמה חלקית |
| 18 | גיבוי ושחזור נתוני אבטחה  | התאמה חלקית |
| 2 | מסמך הגדרות המאגר | התאמה מלאה |
| 2 | בחינה שנתית של כמות המידע הנשמר במאגר  | התאמה מלאה |
| 3 | ממונה על אבטחת מידע  | התאמה מלאה |
| 4 | נוהל אבטחה | התאמה מלאה |
| 5 | מיפוי מערכות המאגר  | התאמה מלאה |
| 5 | ביצוע סקרי סיכונים ומבדקי חדירה למאגרים ברמת אבטחה גבוהה ובינונית  | התאמה מלאה |
| 6 | אבטחה פיזית וסביבתית  | התאמה מלאה |
| 7 | אבטחת מידע בניהול כוח אדם  | התאמה מלאה |
| 7 | ביצוע הדרכות בנושא פרטיות  | התאמה מלאה |
| 9 | זיהוי ואימות  | התאמה מלאה |
| 13 | הפרדה בין מערכות המאגר למערכות מחשוב אחרות  | התאמה מלאה |
| 13 | עדכונים שוטפים של מערכות המאגר | התאמה מלאה |
| 14 | חיבור מאובטח לרשת האינטרנט ובגישה מרחוק  | התאמה מלאה |
| 16 | ביקורות תקופתיות  | התאמה מלאה |
| 19 | חובות בעל המאגר | התאמה מלאה |
| 15 | מיקור חוץ  | לא רלוונטי |

## סיכום ומסקנות

הארגון משקיע משאבים רבים עבור אבטחת המידע בארגון בכלל ועבור עמידה בחוק הגנת הפרטיות בפרט. קיימים נושאים שעל הארגון לתת את דעתו עליהם ובכללם עניין תיעוד הגישה לבסיסי נתונים.

# פירוט הממצאים

## סעיף 2א ו-2ב: מסמך הגדרות המאגר

* פירוט הדרישה: כתיבת מסמך הגדרות לכל מאגר מידע המפרט את הנושאים אשר נקבעו בתקנות (מפורטים מטה) ועדכונו על בסיס שנתי וכן כאשר נעשה שינוי משמעותי באחד מן הנושאים המצוינים בתקנה, בוצעו שינויים טכנולוגיים ארגונים או בהתרחשות אירוע אבטחה.
* רמת תאימות: התאמה מלאה
* תיאור המצב הקיים:
* לXXX שני מאגרי מידע אשר רשומים במשרד המשפטים: מאגר העובדים והמאגר הסטטיסטי. לשני מאגרים אלו קיימים מסמך הגדרות מאגר.

## סעיף 2ג: בחינה שנתית של כמות המידע הנשמר במאגר

* פירוט הדרישה: בעל המאגר יבחן אחת לשנה האם המידע הנשמר במאגר אינו רב מהנדרש לקיום מטרות המאגר.
* רמת התאימות: התאמה מלאה
* תיאור המצב הקיים:
* הסטטיסטיקאים מבצעים בדיקות תקינות על השדות המתקבלים מעת לעת ומתוקף עבודתם.
* בעת הגשת בקשה לחידוש – מבוצעת בדיקת הכרח של שדות המתבקשים, בן מצד הXXX והן מצד הרשות.

## סעיף 3: ממונה על אבטחת מידע

* פירוט הדרישה: מינוי גורם הממונה על אבטחת מידע או ממונה אל אבטחת מידע במאגרי המידע אשר יהיה כפוף ישירות למנהל המאגר, מנהל פעיל של בעל המאגר או המחזיק או לנושא משרה בכירה אחר הכפוף ישירות למנהל המאגר.
* רמת תאימות: התאמה מלאה
* תיאור המצב הקיים:
* קיימת הפרדה בין מנהל אבטחת המידע לבין ממונה אבטחת המידע וכן יש הגדרת תפקידים שונה: קיים ממונה אבטחת מידע, ראש תחום יישומי אבטחת מידע ו-CISO.

## סעיף 4: נוהל אבטחה

* פירוט הדרישה: הכנת נוהל אבטחת מידע למאגרי המידע אשר יתייחס לנושאים שנקבעו בתקנה (מפורטים מטה).
* רמת תאימות: התאמה מלאה
* תיאור המצב הקיים:
* הוגדר נוהל אבטחה כנדרש בתקנות. נוסף לכך, הארגון תשתית נוהלית להסמכה לתקן 27001, ביניהם גם נוהל אבטחת מידע.

## סעיף 5א: מיפוי מערכות המאגר

* פירוט הדרישה: הכנת מסמך מעודכן של שמה מאגרי המידע ורשימת מצאי מעודכנת של מערכות המאגר.
* רמת תאימות: התאמה מלאה
* תיאור מצב קיים:
* יש מסמך ארכיטקטורה של הרשת, מיפוי מסדי הנתונים כולל מנהלי מסדי הנתונים, וכן עובדים עם תוכנה ייעודית לזיהוי המצאי.

## סעיף 5ג ו-5ד:ביצוע סקרי סיכונים ומבדקי חדירה למערכות המאגרים ברמת אבטחה גבוהה

* פירוט הדרישה: ביצוע סקר לאיתור סיכוני אבטחת מידע (סקר סיכונים) אחת לשמונה עשר חודשים וביצוע דיון בתוצאות הסקר שבסיכומו יעודכן מסמך הגדרות המאגר בהתאם לצורך ויבוצעו פעולות לתיקון הליקויים.
* רמת תאימות: התאמה מלאה
* תיאור מצב קיים:
* בוצעו לאחרונה מבדקי חדירה פנימיים וחיצוניים.
* בוצעו סקרי סיכונים על ידי יועץ חיצוני, האחרון בוצע לפני שלושה חודשים.

## סעיף 6א: אבטחה פיזית וסביבתית

* פירוט הדרישה: מערכות המאגר יישמרו במקום מוגן המונע חדירה וכניסה ללא הרשאה. באתרים בהם נשמרות מערכות התומכות במאגרי מידע ברמת אבטחה בינונית או גבוהה יש להתקין אמצעים לבקרה ותיעוד של כניסה ויציאה.
* רמת תאימות: התאמה מלאה
* תיאור מצב קיים:
* חדרי השרתים מוגנים באמצעות כניסה ביומטרית. קיימת בקרת אקלים ורצפה צפה בחדר השרתים.
* הכניסה למתחם נעשית באמצעות כרטיס עובד. ההרשאות בכרטיס העובד ניתנות על ידי הקב"ט.
* יש מאבטח 24/7 למתחם.
* קיימת אזעקה לארונות התקשורת.

## סעיף 7א: אבטחת מידע בניהול כוח אדם

* פירוט הדרישה: הגדרת תהליך מיון וגיוס עובדים התואם את רמת רגישות המידע אליו יחשפו במהלך עבודתם.
* רמת תאימות: התאמה מלאה
* תיאור מצב קיים:
* הגיוס מבוצע דרך מכרזים.
* כיוון שהגוף הינו גוף תמ"ק, כל עובדי הלשכה עוברים סיווג. עובדי הלשכה מסווגים לרמה 6. עובדי IT מסווגים לרמה 4 ותפקידים בכירים יסווגו לרמה 3.

## סעיף 7ב: ביצוע הדרכות בנושא פרטיות

* פירוט הדרישה: קיום הדרכות תקופתיות בנושא פרטיות ואבטחת מידע לבעלי הגישה למאגרים ברמת אבטחה בינונית וגבוהה.
* רמת תאימות: התאמה מלאה
* תיאור מצב קיים:
* נעשות הדרכות אבטחת מידע והדגשה של מאגרי המידע.
* כל עובד עובר תדרוך אבטחת מידע אישי בעת הגעתו לXXX.
* פעם בשנה מועברת הדרכת מודעות לאבטחת מידע.

## סעיף 8: ניהול הרשאות גישה

* פירוט הדרישה: קביעת הרשאות גישה למערכות המאגר בהתאם להגדרות התפקיד ובהתאם לעקרון "הצורך לדעת". ניהול רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ובעלי ההרשאות הממלאים את התפקיד.
* רמת תאימות: התאמה מלאה
* תיאור מצב קיים:
* הרשאות הגישה ניתנות על בסיס הצורך לדעת (Need To Know Basis).
* קיים סבב אישורים לאישור הרשאות.
* ההרשאות ניתנות לפי פרופיל הרשאות.

## סעיף 9: זיהוי ואימות

* פירוט הדרישה: קיום בקרות על גישה למאגר ולמערכות המאגר.
* רמת תאימות: התאמה מלאה
* תיאור מצב קיים:
* מבוצעת סקירת הרשאות תקופתית.
* קיימת מדיניות גישה הכוללת ניתוק אוטומטי של 15 דקות, קיים חיוב להחליף סיסמא כעבר 90 יום.
* הגישה אינה באמצעות הזדהות חזקה.
* נוהל האבטחה מכיל התייחסות למדיניות הגישה ולחוזק הסיסמאות.
* קיים תהליך מסודר להסרת הרשאות בעת עזיבת עובד הכולל תשאול אצל מנהל אבטחת המידע.

## סעיף 10: בקרה ותיעוד גישה

* פירוט הדרישה: הטמעת מנגנון בקרה אשר יתעד באופן אוטומטי ביקורת על הגישה למערכות המאגר ברמת אבטחה גבוהה או בינונית לרבות נתונים אודות זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכבי המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה והאם אושרה או נדחתה.
* רמת תאימות: התאמה חלקית
* תיאור הממצא:
* לא מבוצע רישום security log בבסיסי הנתונים של מערכות המאגר (מי ניגש, מתי, מה ביצע וכו').
* המלצות:
* יש להוסיף יכולות תמיכה בsecurity logs(ניסיונות גישה למערכות המאגר) לבסיסי הנתונים.
* יש להגדיר בנוהל האבטחה את דרישות הניטור במאגרים וליישם ניטור בפועל בהתאם.
* יש להקצות כוח אדם לביצוע מעבר ובקרה שוטפים על לוגים.

## סעיף 11א: תיעוד של אירועי אבטחה

* פירוט הדרישה: יש להטמיע מנגנון לתיעוד אירועים המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה. ככל הניתן התיעוד יבוסס על רישום אוטומטי.
* רמת תאימות : אין התאמה
* תיאור הממצא:
* המחשב אינו מחובר למערכת מרכזית (כגון SIEM) לתיעוד אירועים אך קיימת תכנית ליישום מערכת זו.
* לא קיים נוהל מוטמע לניהול אירועי אבטחת מידע, עם זאת אירועי אבטחה מתועדים ונידונים ברמה תוך מחלקתית.
* המלצות:
* יש לקדם חיבור מערכות הארגון למערכת מרכזית לניהול אירועים SIEM SOC באתר או מנוהל כשירות.
* יש לקבוע שיטה לתיעוד מסודר של אירועים.
* יש להטמיע נוהל לניהול ותיעוד אירועים.

## סעיף 12: התקנים ניידים

* פירוט הדרישה: יש להגביל או למנוע אפשרות לחיבור התקנים ניידים למערכות המאגר בהתאם לרמת אבטחת המידע, רגישות המידע במאגר, ניתוח הסיכונים כתוצאה מחיבור זה ואמצעי ההגנה הקיימים למולם.
* רמת תאימות: התאמה חלקית
* תיאור הממצא:
* כל תחנות הקצה מוגבלות על ידי מערכת להגבלת התקנים.
* קיימת מדיניות למדיה נתיקה.
* קיימת רשימה מצומצמצץ של אנשים אשר מותר להם להשתמש בהתקנים ניידים.
* אין חסימת התקנים ניידים ברמת השרתים.
* המלצות:
* יש לוודא כי בכלל השרתים מבוצעת חסימה של חיבור התקנים ניידים.

## סעיף 13ב: הפרדה בין מערכות המאגר למערכות מחשוב אחרות

* פירוט הדרישה: הפרדה בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר.
* רמת תאימות: התאמה מלאה
* תיאור הממצא:
* מבוצעת הפרדה בין מערכות המאגר למערכות אחרות.

## סעיף 13ג: עדכונים שוטפים של מערכות המאגר

* פירוט הדרישה: ביצוע עדכונים שוטפים למערכות המאגר לרבות חומרה. הימנעות משימוש ממערכות EOL (end of life).
* רמת תאימות: התאמה מלאה.
* תיאור הממצא:
* יש מדיניות התקנת טלאים.
* העדכונים מבוצעים באמצעות מערכת WSUS.
* עדכוני תחנות הקצה נעשה אחת לחודש ועדכון השרתים נעשה אחת לרבעון.
* מבוצעות בדיקות דלתאות יומיים לאחר התקנת העדכונים.

## סעיף 14: חיבור מאובטח לרשת האינטרנט ובגישה מרחוק למערכות המאגר

* פירוט הדרישה: התקנת אמצעי הגנה מתאימים למערכות המאגר המחוברות לרשת האינטרנט. במאגרים אשר ניתן לגשת אליהם מרחוק, התקנת אמצעי אבטחה שמטרתם ביצוע זיהוי ואימות של מבקש הגישה.
* רמת תאימות: התאמה מלאה
* תיאור הממצא:
* קיימת הפרדה מלאה בין רשת האינטרנט לבין רשת המאגר.
* אין גישה מרחוק לרשת המאגר.

## סעיף 15: מיקור חוץ

* פירוט הדרישה: ביצוע הערכת סיכונים טרם התקשרות עם ספק בעל גישה למערכות ה-IT והגדרת הנושאים הקבועים בתקנה במסגרת חוזה ההתקשרות.
* רמת תאימות: לא רלוונטי
* תיאור הממצא
* לא מתקיימת עבודה עם מיקור חוץ בהקשרי העברת המידע.

## סעיף 16: ביקורות תקופתיות

* פירוט הדרישה: במאגרי מידע ברמת אבטחה בינונית או גבוהה יש לבצע אחת לשנתיים ביקורת אבטחה פנימית או חיצונית לבחינת עמידה בהוראות התקנות, על ידי גורם בעל הכשרה מתאימה.
* רמת תאימות: התאמה מלאה
* תיאור מצב קיים:
* הארגון מלווה ביועץ חיצוני לבחינת עמידה בחוק, המבצע ביקורות עצמיות.

## סעיפים 17 ו-18: שמירת נתוני אבטחה וביצוע גיבוי ושחזור לנתונים

* פירוט הדרישה: שמירת נתוני אבטחה באופן מאובטח למשך 24 חודשים וגיבוי נתוני אבטחה באופן שניתן יהיה לבצע שחזור של הנתונים בכל עת.
* רמת תאימות: התאמה חלקית
* תיאור מצב קיים:
* נתוני האבטחה אינם נשמרים למשך 24 חודשים.
* המידע ברשת מגובה ושחזורים יזומים מבוצעים אחת לשבוע.
* לא קיים עותק גיבוי לנתונים.
* המלצות
* יש לוודא כי נתוני האבטחה המוגדרים בתקנות נשמרים לפרק הזמן המוגדר בתקנות ומגובים כנדרש.
* יש לוודא כי אתר עותק גיבוי.

## סעיף 19: תיעוד חובות בעל המאגר

* פירוט הדרישה: כל מי שמוטלת עליו חובה לביצוע – בעל מאגר, מנהל מאגר או מחזיק, יש לתעדה.
* רמת תאימות: התאמה מלאה
* תיאור מצב קיים:
* הארגון נעזר במחלקה משפטית המלווה אותו לעמידה בחוק וכן ביועץ חיצוני לענייני הגנת הפרטיות ואבטחת מידע.
* קיים מסמך תיעוד חובות בעל המאגר ומנהלי המאגר.