**ביקורת תאימות**

**תקנות הגנת הפרטיות**

**חברת XXX**

**רשות האוכלוסין וההגירה**

**11/12/2018**

**© 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 רשות האוכלוסין, אגף אבטחת מידע.

### תוכן עניינים

1. תמצית מנהלים 3

1.1. רקע 3

1.2. על החברה 3

1.3. עיקרי הממצאים: 4

1.4. סיכום ומסקנות: 6

2. פירוט הממצאים 6

2.1. סעיף 2א ו-2ב: מסמך הגדרות המאגר 6

2.2. סעיף 2ג: בחינה שנתית של כמות המידע הנשמר במאגר 6

2.3. סעיף 3: ממונה על אבטחת מידע 7

2.4. סעיף 3(3) תכנית עבודה לבקרה על העמידה בדרישות: 7

2.5. סעיף 4: נוהל אבטחה 7

2.6. סעיף 5: מיפוי מערכות המאגר 8

2.7. סעיף 5ג ו-5ד:ביצוע סקרי סיכונים ומבדקי חדירה למערכות המאגרים ברמת אבטחה גבוהה 8

2.8. סעיף 9ב: בקרת גישה 8

2.9. סעיף 10: בקרה ותיעוד גישה 9

2.10. סעיף 11א: תיעוד של אירועי אבטחה 9

2.11. סעיף 12: התקנים ניידים 9

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

2.13. סעיף 14: מדיניות הצפנה למאגרים 10

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

2.15. סעיפים 19: חובות בעל המאגר 10

# תמצית מנהלים

## רקע

במהלך חודש אוקטובר 2018 ביצעה חברת 2bsecure סקר אצל לקוחות חיצוניים מטעם רשות האוכלוסין בחברת XXXXXX. 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 בעמידתו של הלקוח החיצוני בתקנות אלו.

חברת XXXXXX מקבלת מרשות האוכלוסין מידע על חייבים של הרשויות איתן היא עובדת.

## על החברה

* חברת XXXXXX (XXX לשעבר) מספקת שירותי מידע עבור העיריות איתן היא עובדת, להשלמת פרטי תושבים לצורך הוצאת שוברי תשלום על דוחות.
* בשנת 2014 התרחש אירוע אבטחת מידע בחברת XXX, אירוע אשר הסתיים לאחר תחקור מקיף ומעמיק וכן שינויים שבוצעו בעקבותיו. לא נגרם נזק משמעותי.
* חברת XXXXXX נקנתה לאחרונה על ידי החברה לXYYY. כחלק מכך, החברה נהנית משירותי התשתית של החברה XXX. החיבור נעשה באמצעות סגמנט עם FW נפרד, השייך לחברת XXXXXX בלבד.
* תחנות העבודה של חברת XXXXXX מחוברות לסגמנט נפרד.
* החברה מקבלת מידע בקבצי batch: שיטת הפעולה מתבצעת על ידי הגשת בקשה הכוללת את פרטי החייבים המכילים מספר תעודת זהות וכתובת. הפרטים האלו נשלחים לחברת HP (רשות האוכלוסין) לבדיקת עדכניות ונכונות. לאחר קבלת הקובץ בחזרה, הקובץ מוזן למערכת על ידי אחד העובדים אשר מעלה את הקובץ מהכספת ונשלחת דרישת תשלום לכתובת המעודכנת והאחרונה כפי שהתקבלה מרשות האוכלוסין.
* מחיקת הקבצים מתבצעת ידנית.
* הקבצים נמצאים על מחשב המחובר באמצעות IPVPN בענן, ללא גישה דרך האינטרנט מהרשת הציבורית.
* חברת XXXXXX מוסמכת לתקן ISO27001. ככזו, חלות עליה הקלות בבחינת סעיפי החוק.

## עיקרי הממצאים:

**נושאים שנמצאו תקינים:**

* החברה נוקטת באמצעים להגנה על מאגריה ומנהלת רישום מאגרים כדין.
* מונה מנהל אבטחת מידע.
* קיימים נהלי אבטחה המתייחסים לחלק נרחב מנושאי אבטחת המידע.
* לא נמצאו פערים בנושא ניהול מאובטח של כוח אדם.

**פערים:**

* לא מבוצעת בחינה תקופתית של השדות המתקבלים על מנת לבחון יתירות של השדות.
* לא מבוצעות הדרכות בנושאי אבטחת מידע והגנת הפרטיות.
* לא מתבצעים סקרי סיכונים ובדיקות חדירות תקופתיים.
* המידע המגובה נשמר לתקופה של שלושה חודשים ולא כנדרש.

**המלצות:**

* יש להגדיר תכנית עבודה רב שנתית לביצוע סקרי סיכונים ו- PT.
* יש לבצע ביקורת לספקי מיקור חוץ הניגשים מרחוק למערכת.
* יש לבצע בחינה של השדות המתקבלים ושל המידע המתקבל ולתעד בדיקה זו.
* יש להוסיף להדרכות המודעות את נושא הגנה על הפרטיות והגנה על מאגרי מידע.
* מומלץ להוסיף תכנית העבודה לאבטחת מידע התייחסות לעמידה בתקנות הגנת הפרטיות: אבטחת מידע.
* מומלץ לתקשר את נהלי אבטחת המידע לכלל העובדים.
* מומלץ להשתמש בכלים להצפנת הקבצים ברשת הפנימית וכן להצפין מחשבים ניידים.
* יש לשמור את המידע המגובה ל-24 חודשים כמפורט בתקנות.
* להלן מפת חום המצביעה על עמידת החברה בתקנות בהתייחסות לרמת בקרות כללית לטכנולוגיה ותהליכי עבודה כלליים. הפירוט הינו לפי רמת התאימות לסעיפים השונים בתקנות, כפי שנדרש מחברה המוסמכת לתקן ISO27001.

|  |  |  |
| --- | --- | --- |
| פרק | נושא | סטאטוס |
| 3 | ממונה על אבטחת מידע | התאמה מלאה |
| 5 | מיפוי מערכות המאגר | התאמה מלאה |
| 9 | זיהוי ואימות | התאמה מלאה |
| 10 | בקרה ותיעוד גישה | התאמה מלאה |
| 11 | תיעוד של אירועי אבטחה | התאמה מלאה |
| 12 | התקנים ניידים | התאמה מלאה |
| ג2 | בחינה שנתית של כמות המידע הנשמר במאגר | התאמה חלקית |
| (3)3 | תכנית בקרה שוטפת לעמידה בתקנות | התאמה חלקית |
| 4 | נוהל אבטחה | התאמה חלקית |
| 5 | ביצוע סקרי סיכונים ומבדקי חדירה למאגרים ברמת אבטחה גבוהה ובינונית | התאמה חלקית |
| 14 | חיבור מאובטח לרשת האינטרנט ובגישה מרחוק | התאמה חלקית |
| 18 | גיבוי ושחזור נתוני אבטחה | התאמה חלקית |
| 2 | מסמך הגדרות המאגר | לא רלוונטי |
| 6 | אבטחה פיזית וסביבתית | לא רלוונטי |
| 7 | אבטחת מידע בניהול כוח אדם | לא רלוונטי |
| 7 | ביצוע הדרכות בנושא פרטיות | לא רלוונטי |
| 8 | ניהול הרשאות גישה | לא רלוונטי |
| 13 | הפרדה בין מערכות המאגר למערכות מחשוב אחרות | לא רלוונטי |
| 13 | עדכונים שוטפים של מערכות המאגר | לא רלוונטי |
| 15 | מיקור חוץ | לא רלוונטי |
| 16 | ביקורות תקופתיות | לא רלוונטי |
| 17 | שמירת נתוני אבטחה | לא רלוונטי |

## סיכום ומסקנות:

כהתייחסות כוללת, החברה נוקטת פעולות לשמירה על אבטחת המידע. המעבר לחברת XYYY מעביר את החברה לעמדה חזקה יותר בהיבטי אבטחת מידע. עם זאת, ישנם מספר דגשים שהחברה צריכה לבחון על מנת לקיים את תקנות אבטחת המידע.

# 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: **לא רלוונטי**
* תיאור המצב הקיים:
* חברת XXXXXX נחשבת כמחזיקת מאגרים מרובים ועל כן אינה רושמת אותם.
* החברה מוחקת את המאגרים המתקבלים מרשות האוכלוסין בסיום העבודה, באופן ידני.

## 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 תאימות: **התאמה חלקית**
* תיאור המצב הקיים:
* ככלל, לא מבוצעת סריקה של השדות המתקבלים, אלא במקרה של קבלת נתונים שגויים יש התראה אשר מונעת מהפעולה להמשיך.
* המידע נמחק ידנית על ידי אחד העובדים.
* המלצות:
* יש לבצע בחינה של המצב הקיים לגבי המידע המתקבל ובמידת הצורך למחוק מידע מיותר. יש לחזור על בחינה זו אחת לשנה לצורך עמידה בדרישת התקנה.
* יש לבצע בחינה של עובדים המטפלים בהורדה והעלאת הנתונים מהכספת לוודא מחיקה של מידע.

## 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.
* לא קיים ניגוד עניינים בין פעילויות מנהל אבטחת מידע ובין פעילויות ממונה אבטחת מידע, לחברת XXXXXX יש מנהל אבטחת מידע ולחברה לXYYY יש מנהל אבטחת מידע.

## סעיף 3(3) תכנית עבודה לבקרה על העמידה בדרישות:

* פירוט הדרישה: ממונה אבטחת מידע יכין תכנית עבודה לביצוע בקרה שוטפת על העמידה בדרישות תקנות אלו.
* רמת תאימות: **התאמה חלקית**
* תיאור המצב הקיים:
* קיימת תכנית עבודה לנושאי אבטחת מידע, אך תכנית זו אינה כוללת התייחסות לתקנות אבטחת המידע.
* המלצה:
* יש לכלול את נושא תקנות הגנת הפרטיות בתכנית העבודה לאבטחת מידע.

## סעיף 4: נוהל אבטחה

* פירוט הדרישה: הכנת נוהל אבטחת מידע למאגרי המידע אשר יתייחס לנושאים שנקבעו בתקנה (מפורטים מטה).
* רמת תאימות: **התאמה חלקית**
* תיאור המצב הקיים:
* הוגדר נוהל אבטחה, נוהל זה טרם תוקשר לכלל העובדים. כרגע בתהליכי תקשור אך טרם הושלם.
* המלצות:
* מומלץ לתקשר את נהלי אבטחת המידע לכלל העובדים ולשמור אותם במקומות נגישים.

## סעיף 5: מיפוי מערכות המאגר

* פירוט הדרישה: הכנת מסמך מעודכן של שמה מאגרי המידע ורשימת מצאי מעודכנת של מערכות המאגר.
* רמת תאימות: **התאמה מלאה.**
* תיאור הממצא
* בוצע מיפוי מערכות ונכסים בהתאם לתקן ISO 27001.

## 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 חלקית**
* תיאור המצב הקיים:
* לא מבוצעים מבדקי חדירה וסקרי סיכונים כל שנתיים, התקנות מנחות לבצע סקרי סיכונים ומבדקי חדירה במערכות המאגרים ברמת אבטחה גבוהה אחת ל 18 חודשים.
* **המלצות**
* יש להגדיר תכנית עבודה רב שנתית לביצוע סקרי סיכונים ו PT לתשתיות המחזיקות את המאגר ולמערכות מאגרי המידע ברמת אבטחה גבוהה אחת ל 18 חודשים.

## סעיף 9ב: בקרת גישה

* פירוט הדרישה: קיום בקרות על גישה למאגר ולמערכות המאגר.
* רמת תאימות: **התאמה מלאה**
* תיאור הממצא:
* קיימת מורכבות הסיסמא
* כל שלושה חודשים יש חיוב להחליף סיסמא
* קיימת הזדהות רב שלבית בעת התחברות מרחוק
* יש מערכת להגנה על תחנות קצה

## 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 מלאה**
* תיאור הממצא:
* נתוני הבקרה מתועדים.

## 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 : **התאמה מלאה**
* תיאור הממצא:
* מבוצע תהליך לתיעוד כחלק מההסמכה לתקן ISO27001.

## 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 מולם.
* רמת תאימות: **התאמה מלאה**
* תיאור הממצא:
* אין הגבלה פיזית על חיבור התקנים ניידים למערכות המחשוב. עם זאת, קיים מוצר הגנה על עמדת קצה אשר אינה מאפשרת חיבור התקנים נתיקים.
* המלצות:
* יש לוודא כי בכלל השרתים מבוצעת חסימה של חיבור התקנים ניידים.

## 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:**
* קיימים אמצעי הגנה בעת חיבור מרחוק.

## סעיף 14: מדיניות הצפנה למאגרים

* פירוט הדרישה: העברת מידע ממאגר המידע תיעשה תוך שימוש בשיטות הצפנה מקובלות.
* **רמת תאימות: התאמה חלקית**
* **תיאור מצב קיים:**
* קיימת הצפנה בגישה מרחוק.
* בתוך הרשת הפנימית אין הצפנה.
* אין הצפנה של מחשבים ניידים.

## 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 הממצא**
* גיבויים מבוצעים לשרתים וירטואליים, ברמת הפלטפורמה מבוצע SNAPSHOT כל שעתיים
* יש אפשרות לחזור אחורה חודש ימים.
* לDB יש גיבוי לשלוח חודשים אחורה.
* **המלצות**
* יש לוודא כי נתוני האבטחה המוגדרים בתקנות נשמרים לפרק הזמן המוגדר בתקנות ומגובים כנדרש.
* הגדרת תכנית שחזורים לכל מערכות המאגרים.
* יש לבצע שמירה של הנתונים ל-24 חודשים.

## סעיפים 19: חובות בעל המאגר

* פירוט הדרישה: קיימות הנחיות לרישום ותפעול חובות בעל המאגר.
* **רמת תאימות: התאמה מלאה**
* **תיאור הממצא**
* בחברה קיימת מחלקת ייעוץ משפטית המלווה ומגדירה את חובות החברה כמחזיקת מאגר.