תאריך הפקה: 16.02.2026

מסמך זה אינו מהווה אסמכתא לשליחת הטופס

שאלון אבטחת מידע- לקוחות חיצוניים

רשות האוכלוסין וההגירה - רשות האוכלוסין

מספר בקשה: 5432

פרטים אודות הלקוח

פרטי איש הקשר

מספר זהות (כולל ספרת ביקורת)

שם פרטי

שם משפחה

דואר אלקטרוני

מייל עבודה

טלפון נוסף

תפקיד איש הקשר

האם איש הקשר זהה לממלא המסמך?

- כן
- לא

פרטי הארגון

מספר לקוח חיצוני

שם הארגון

העברת מידע ללקוח

חשיפת מידע לצד ג'

גוף צד ג'

כל גוף המסייע ללקוח ומאחסן/ מעבד/ מטפל וחשוף למידע המתקבל מרשות האוכלוסין.

האם הלקוח עושה שימוש בצד ג' (כמוגדר לעיל)

- כן
- לא

טבלת פירוט שימוש בצד ג'

צד ג' 1

שם מלא ומדויק של גוף צד ג'

פירוט הפעולות שצד ג' מבצע עבור הלקוח

ממשקי קבלת מידע מרשות האוכלוסין

ממשקי מסירת מידע
מערכת WEB (גחלת)- מערכת שאילתות אינטראקטיבית.
ממשק קבצים- קבלת מידע באמצעות קובץ הנשלח ללקוח (Batch).
API - ממשק מערכת של הלקוח מול מערכות רשות האוכלוסין.

אופן קבלת המידע

קבוצת לקוחות

הערות
כל גוף המבקש לקבל מידע מרשות האוכלוסין נדרש לבצע תהליך בקשת אישור אבטחת מידע וקבלת אישור - גוף כזה מוגדר "לקוח". לכל לקוח יש מספר לקוח (אשר נקבע ע"י רשות האוכלוסין)
עם זאת, יתכן שבפועל שניים או יותר מהלקוחות הינם זהים (לפחות מבחינת דרישות אבטחת מידע). שני לקוחות נחשבים זהים מבחינת דרישות אבטחת מידע במידה שאילו כל אחד היה מגיש מסמכי דרישות אבטחת מידע (כמתואר במסמך זה), הרי המסמכים היו זהים. להלן דוגמאות של נושאים שצריכים להיות זהים ע"מ לקבוע ששני לקוחות זהים:
1. שני הגופים עושים שימוש באותה תשתית סב"ר (סביבת רשת) - קרי, רשת מחשב לרבות שימוש באותם שרתים זהה, באותן עמדות קצה, טכנולוגיות משותפות, אמצעי אבטחת מידע זהים, אמצעי בקרה וניטור זהים וכיוב'.
2. שני הגופים פועלים תחת אותם נהלי אבטחת מידע ומדיניות אבטחת מידע
3. שני הגופים פועלים תחת אותה מעטפת אבטחה פיזית.
4. קיימת תוכנית מודעות/הדרכה זהה/ דומה לשני הגופים

שניים או יותר לקוחות זהים (כמוגדר לעיל) מהווים קבוצת לקוחות.

האם ארגונכם שייך לקבוצת לקוחות

- ○ כן
- ● לא

רמת יישום

לידעתך,
גיליון זה מתייחס לדרישות הטכנולוגיות מלקוח המבקש לקבל מידע מרשות האוכלוסין לרבות הממשקים שלו לגופי צד ג'. אישור אבטחת מידע, במידה שיינתן, יכלול אישור עבודה עם גופי צד ג' המפורטים בפנייה זו.

בשאלות הבאות יש לציין עבור כל שאלה את רמת היישום לפי הפירוט הבא:

התאמה מלאה- הדרישה מיושמת באופן מלא.
התאמה חלקית- הדרישה אינה מיושמת באופן מלא.
אין התאמה- הדרישה אינה מיושמת כלל.
לא רלוונטי- שימוש בערך מוגבל למקרים בהם יישום הסעיף אינו יכול להתקיים במציאות האמורה. לדוגמה: דרישות בריחים בחלונות במבנה שאין לו חלונות, לא רלוונטי.

במידה והנך מתבקש לספק תאריך התחייבות ליישום מלא של הסעיף, יש לציין תאריך סביר להשלמת הדרישה.

1. עובדים בארגון

שאלה 1
בכל ארגון ימונה בעל תפקיד מטעמו שיהיה אמון על נושאי אבטחת המידע וניהולה בהיבטי המידע המתקבל מהרשות. בעל תפקיד זה יהיה בעל הכשרה וניסיון בתחום אבטחת המידע שיאפשרו לו למלא את תפקידו בצורה ראויה.

רמת יישום

שאלה 2
טרם קליטתו לארגון, הארגון מקיים הליך סינון המבטיח מהימנות תעסוקתית של העובד.

רמת יישום

שאלה 3

הגישה למידע תאושר אך ורק לעובד הנושא בתפקיד אשר אושר כמפורט במסמך האישור מראש על ידי הרשות ב "וועדה להעברת מידע".

רמת יישום

שאלה 4

בארגון מתקיימים מעגלי אבטחה פיזיים (כגון: שומר, אזעקה, בקרת כניסה, מצלמות, דלתות, מנעולים וכיוב') המבטיחים זיהוי מקדים ומניעת גישה של גורם שאינו מורשה מלגשת למידע המתקבל מרשות האוכלוסין וההגירה.

רמת יישום

2. תהליכים בארגון

שאלה 1

עובדי הארגון עוברים הכשרה מסודרת ועתית בנושאי אבטחת מידע והגנת הפרטיות.

רמת יישום

שאלה 2

הארגון מנהל תהליך סדור לשמירת הנתונים הנדרשים לטובת הפעילות העסקית בלבד. נתונים עודפים נמחקים מיידית.

רמת יישום

שאלה 3

הארגון מיישם תהליכי עבודה מסודרים המעוגנים בנהלי עבודה, וכן תהליכי העבודה יבטיחו כי קיימת מסגרת ברורה לניהול התקין של המידע המתקבל מהרשות.

רמת יישום

שאלה 4

בארגונים בהם קיים צבר (מ 100,000 רשומות ומעלה) של מידע הארגון ינהל ביקורות עיתיות על ידי בעל מקצוע בתחומי אבטחת המידע/ מערכות מידע אחת ל-18 חודשים לכל היותר. הביקורת תבחן את יישום תהליכי העבודה של הארגון, יישום הנהלים בתחומי אבטחת המידע, יישום עקרונות מעגלי האבטחה שבמסמך זה והניהול השוטף של המידע המתקבל מהרשות.

רמת יישום

שאלה 5

הארגון מיישם מדיניות ארגונית בתחומי הגנת הפרטיות וצנעת הפרט תוך מתן דגש על ניהול מאגרי מידע על פי חוק הגנת הפרטיות, תקנותיו ושאר חוקים רלוונטיים אחרים ומודעות עובדים לנושא.

רמת יישום

טכנולוגיה

3. ניהול הרשאות ובקרת גישה

שאלה 1

הרשאות חזקות למערכות המחשב ניתנות לבעלי תפקידים ייעודים ונערכת בקרה עתית אחר הצורך של העובד בהרשאה.

רמת יישום

שאלה 2

על הארגון לוודא כי הרשאות למידע ניתנות על פי העקרונות "הצורך לדעת" ועיקרון- "הרשאות מינימאליות". כלומר- הרשאות למידע מוענקות לעובד על בסיס תפקיד, אחריות ומילוי חובתו בתוקף תפקידו בלבד וללא הרשאות עודפות שאינן נדרשות לעובד באופן שוטף ומתקיימת בקרה עיתית לתיקוף ההרשאות.

רמת יישום

שאלה 3

הארגון מממש שימוש ברכיבים להבטחת זהותם של העובדים ואשר כוללים הזדהות מרובת גורמים (2FA\MFA)

רמת יישום

שאלה 4

חשבון משתמש ייחסם לאחר מספר מוגדר של ניסיונות כניסה כושלים (לא יעלה על 10).

רמת יישום

שאלה 5

חיבור משתמש למערכת (Session) ייסגר (Logout) לאחר פרק זמן של חוסר פעילות(עד שעה).

רמת יישום

שאלה 6

הארגון מנהל את מחזור חיי המשתמש במערכות הארגון, ומבטל חשבונות משתמשים שאינם פעילים במערכת לאורך תקופה.

רמת יישום

4. תקשורת

שאלה 1

העברת המידע שהגיע מרשות האוכלוסין בין אתרים של הארגון מבוצעת באופן מוצפן המבטיח כי גורם שאינו מורשה לא יוכל להיחשף למידע בעת העברתו. לרבות תקשורת עם צד ג' במידה וקיימת.

רמת יישום

שאלה 2

הארגון מנהל אבטחת מנגנוני גישה בתקשורת באמצעות ניהול מסודר ועדכני של רכיב לסינון ובקרת תקשורת כדוגמת "חומת אש" (Firewall).

רמת יישום

שאלה 3

בארגונים בהם קיים צבר (מ 100,000 רשומות ומעלה) של מידע, הארגון ינהל הפרדה (סגמנטציה) ברשת המבטיחה הפרדה ברמת התקשורת בין סביבות העבודה השונות בארגון לבין הסביבה המכילה את המידע המתקבל מרשות האוכלוסין.

רמת יישום

שאלה 4

בארגונים בהם קיים צבר (מ 100,000 רשומות ומעלה) של מידע, יממש הארגון שימוש במנגנוני ניטור ובקרה לזיהוי תקשורת חריגה בתעבורת הרשת ו/או התחנה כדוגמת IDS ו/או IPS.

רמת יישום

5. הגנה על בסיס נתונים

שאלה 1

בארגונים בהם קיים צבר רב (500,000 רשומות ומעלה) של מידע, יממש הארגון הגנה על בסיס הנתונים באמצעות רכיב בקרת תקשורת וגישה כדוגמת DBF (חומת אש לבסיסי נתונים).

רמת יישום

שאלה 2

הארגון עושה שימוש באמצעים למניעת וירוסים כדוגמת "אנטי וירוס" (AV) /EDR מעודכן ופעיל.

רמת יישום

שאלה 3

הארגון מממש הגבלת הגישה למינימום הנדרש למנהלי בסיסי הנתונים ושאר בעלי הרשאות גבוהות.

רמת יישום

שאלה 4

הארגון מנהל באופן תדיר וסדור עדכונים עבור תוכנות מערכות הפעלה ועדכון גרסאות תוכנה

רמת יישום

6. סיסמאות

שאלה 1

מערכות המחשב מחייבות שימוש בסיסמה.

רמת יישום

שאלה 2

מערכות המחשב מחייבות החלפת סיסמה עתית(עד חצי שנה).

רמת יישום

שאלה 3

מערכות המחשב מחייבות שימוש בסיסמה מורכבת.

רמת יישום

7. הגנה על תחנות קצה

שאלה 1

הארגון עושה שימוש באמצעים להגנה על תחנות הקצה מפני אמצעים נתיקים **לא מורשים**.

רמת יישום

שאלה 2

בעת חיבור אמצעים נתיקים מורשים הארגון מבצע סריקת "אנטי וירוס" לגילוי וחסימת פוגענים.

רמת יישום

8. אחסון וניטור

שאלה 1

אחסון נתונים שהתקבלו מרשות האוכלוסין באמצעים נתיקים מחייב גריטתם באופן מסודר על ידי גריסתם ו/או התכתם כך שלא יהיה ניתן לשחזר מהם מידע.

רמת יישום

שאלה 2

הארגון מנהל תהליך של בקרה וניטור אחר ניהולו של המידע המתקבל מהרשות. תהליך הבקרה והניטור ישמש ככלי שליטה בידי הארגון לנעשה עם המידע.

רמת יישום

העברת מידע לחו"ל

האם הגוף מעביר/מאחסן מידע שמקורו מרשות האוכלוסין אל מחוץ לגבולות ארץ ישראל, לרבות אחסון בענן, עיבוד בענן וכד.

- ◯ כן
- ◯ לא

מועד שליחת הטופס

תאריך

[redacted]

הטופס מיועד לשני המינים כאחד, אך לעיתים מנוסח בלשון זכר או נקבה.

טופס זה מכיל מידע מוגן על פי חוק הגנת הפרטיות.